รายงานการวิจัยฉบับสมบูรณ์

โครงการศึกษาและทดสอบ
Cyber Threat intelligence Feeds หลายแหล่ง
เพื่อปรับใช้กับระบบข่าวกรองภัยคุกคามทางไซเบอร์แบบไม่เสียค่าใช้จ่าย

โดย

ศูนย์ไซเบอร์กองทัพอากาศ

มีนาคม ๒๕๖๘

บทคัดย่อ

โครงการวิจัยเรื่อง ศึกษาและทดสอบ Cyber Threat Intelligence Feeds หลายแหล่ง เพื่อปรับใช้กับระบบข่าวกรองภัยคุกคามทางไซเบอร์แบบไม่เสียค่าใช้จ่าย

นายทหารโครงการ นาวาอากาศโท บุรีรัตน์ เข็มทอง

หน่วยเจ้าของโครงการ ศูนย์ไซเบอร์กองทัพอากาศ

ในปัจจุบัน หน่วยงานด้านความมั่นคงมีการประยุกต์ใช้งานระบบข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence) จากหลายแหล่ง เพื่อใช้ในการตรวจสอบภัยคุกคามไซเบอร์ โดยข้อมูลข่าวกรองดังกล่าวประกอบด้วย ฐานข้อมูลเว็บไซต์ ยูอาร์แอล ข้อมูลมัลแวร์ หมายเลขไอพีอันตรายที่ผ่านการตรวจสอบแล้วว่าเป็นกลุ่มไอพีที่ถูกแฮกเกอร์ใช้เป็นเครื่องมือในการโจมตีหรือสร้างความเสียหายให้กับเครือข่าย และข้อมูลการโจมตีเหล่านี้มีการเผยแพร่สู่สาธารณะตามแหล่งข้อมูลที่เรียกกันว่า Blacklist IP หรือข้อมูลช่องโหว่ ซึ่งถือเป็นข้อมูลสำคัญที่สามารถใช้ในการบ่งชี้ว่าระบบถูกโจมตีหรือถูกบุกรุกซึ่งถูกเรียกว่า IOCs (Indicator of Compromise) โดยฐานข้อมูลเหล่านี้ สามารถนำมาปรับปรุงพัฒนา การเฝ้าระวัง ตรวจจับ แจ้งเตือน และวิเคราะห์ภัยคุกคามทางไซเบอร์ เพื่อให้หน่วยงานสามารถรับมือกับภัยคุกคามเหล่านั้นได้อย่างทันท่วงทีและป้องกันไม่ให้เกิดความเสียหายที่ร้ายแรง

ดังนั้นงานวิจัยนี้จึงมุ่งพัฒนาระบบและกระบวนการตรวจสอบข้อมูลภัยคุกคามจากหลายแหล่งที่มา เพื่อเพิ่มความน่าเชื่อถือของข้อมูลที่ถูกนำไปใช้ในการนำไปวิเคราะห์และเฝ้าระวังการโจมตีจากภัยคุกคามทางไซเบอร์ อีกทั้งยังสามารถแจ้งเตือนการโจมตีของภัยคุกคามที่เกิดขึ้น ทำให้สามารถประเมินเหตุการณ์ สามารถคาดคะเน รวมถึงประเมินสถานการณ์เกี่ยวกับภัยคุกคามที่หน่วยงานกำลังเผชิญอยู่ รวมถึงการสืบสวนหาบุคคลผู้อยู่เบื้องหลัง วัตถุประสงค์ แรงจูงใจ และเป้าหมายในการคุกคามต่อระบบ รวมถึงวิเคราะห์ระบบภายในหน่วยงานที่อาจเป็นเป้าหมายที่ถูกโจมตีได้อย่างมีประสิทธิภาพ อีกทั้งยังเป็นการนำเสนอตัวแบบ (Prototype) แนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศที่สามารถรับมือกับภัยคุกคามทางไซเบอร์ในอนาคตและสอดรับกับยุทธศาสตร์และนโยบายระดับชาติ และตอบโจทย์ภารกิจ ของกองทัพอากาศ

คำนำ

กองทัพอากาศดำรงวิสัยทัศน์ “กองทัพอากาศชั้นนำในภูมิภาค” โดยมิติไซเบอร์ (Cyber Domain) ถือเป็นหนึ่งมิติทางการรบที่มีความสำคัญ เพราะเป็นมิติที่ครอบคลุมและมีส่วนเกี่ยวข้องกับทุกมิติทางการรบ โดยในปัจจุบันด้วยความรุดหน้าทางเทคโนโลยี ได้ทำให้เกิดความท้าทายต่อความมั่นคงในมิติด้านไซเบอร์ เช่น ภัยคุกคามรูปแบบใหม่ที่มีแนวโน้มพัฒนารุดหน้าและมีความหลากหลายมากขึ้น ทำให้หน่วยงานด้านความมั่นคง โดยเฉพาะศูนย์ไซเบอร์กองทัพอากาศที่เป็นหน่วยงานรับผิดชอบในการดูแลความมั่นคงปลอดภัยไซเบอร์ทั้งเชิงรุกและเชิงรับต้องพัฒนาองค์ความรู้ นวัตกรรม และงานวิจัยเพื่อรองรับต่อภัยคุกคามดังกล่าว

งานวิจัยนี้เป็นส่วนหนึ่งของการพัฒนาต้นแบบในการตรวจจับภัยคุกคามทางไซเบอร์โดยใช้การบูรณาการข้อมูลด้านการข่าวกรองไซเบอร์ผ่านการสร้างระบบในการรวบรวม ประมวลผล วิเคราะห์ข่าวกรองภัยคุกคามด้านไซเบอร์ และทำการรับประเมินแนวทางการรับมือที่เหมาะสม โดยผู้วิจัยหวังเป็นอย่างยิ่งว่า ผลงานวิจัยนี้จะเป็นประโยชน์และเป็นแนวทางในการนำไปใช้งานภายในศูนย์ไซเบอร์กองทัพอากาศ และสามารถใช้เป็นต้นแบบในการจัดทำระบบข่าวกรองทางไซเบอร์เพื่อการเฝ้าระวังในของหน่วยขึ้นตรงกองทัพอากาศต่อไปในอนาคต

กิตติกรรมประกาศ

คณะผู้วิจัยขอขอบคุณ กองทัพอากาศที่ได้กำหนดยุทธศาสตร์กองทัพอากาศ ๒๐ ปีซึ่งอยู่บนพื้นฐานของการให้ความสำคัญในการพัฒนาขีดความสามารถด้านมิติไซเบอร์โดยเฉพาะด้านการวิจัยและพัฒนา คณะผู้บังคับบัญชาระดับสูงของกองทัพอากาศที่ได้เล็งเห็นถึงความสำคัญและอนุมัติให้คณะผู้วิจัยได้ดำเนินการวิจัยนี้ นอกจากนี้ คณะผู้วิจัยขอขอบคุณศูนย์ไซเบอร์กองทัพอากาศที่ให้การสนับสนุนทรัพยากร เวลา และบุคลากร ในการดำเนินการวิจัยและคณาจารย์โรงเรียนนายเรืออากาศนวมินทกษัตริยาธิราชทุกท่านที่ให้ความร่วมมือในการดำเนินการวิจัยเป็นอย่างดี

สารบัญ

สารบัญ (ต่อ)

สารบัญภาพ

สารบัญภาพ (ต่อ)

บทที่ ๑
บทนำ

๑. หลักการและเหตุผล

ภัยคุกคามทางไซเบอร์ (Cyber Threat) มีแนวโน้มความรุนแรงที่ส่งผลกระทบต่อชีวิตและทรัพย์สินมากขึ้นตามลำดับอย่างหลีกเลี่ยงไม่ได้ นอกจากนี้ยังส่งผลกระทบต่อระบบโครงสร้าง พื้นฐานสำคัญของประเทศ (Critical Infrastructure) ได้แก่ กลุ่มโครงสร้างพื้นฐานสำคัญของประเทศ เช่น กลุ่มความมั่นคงและบริการภาครัฐ กลุ่มการเงิน กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม กลุ่มการขนส่งและโลจิสติกส์ กลุ่มพลังงานและสาธารณูปโภค กลุ่มสาธารณสุข เป็นต้น ส่งผลกระทบต่อความมั่นคงปลอดภัยของประเทศในภาพรวม จะเห็นได้ว่า ภัยคุกคามทางไซเบอร์เป็นภัยคุกคามรูปแบบใหม่ ที่เน้นกระทำต่อ ระบบอินเทอร์เน็ต และระบบเครือข่ายคอมพิวเตอร์ ทำให้ประชาคมโลกเริ่มตื่นตัวและตระหนักถึงภัยคุกคามดังกล่าว ตัวอย่าง ภัยคุกคามทางไซเบอร์ที่โจมตีโครงสร้างพื้นฐานสำคัญในระดับโลก เช่น เหตุการณ์ทาง ไซเบอร์ที่เพิ่งเกิดขึ้นคือ บริษัท Colonial Pipeline ฝั่งตะวันออกของสหรัฐอเมริกาโดนโจมตีด้วยโปรแกรมประสงค์ร้ายเรียกค่าไถ่ (Ransomware) โดยยึดข้อมูลเกือบ ๑๐๐ กิกะไบต์เป็นประกัน[๒] ทำให้ระบบการขนส่งน้ำมันผ่านท่อลำเลียงล่ม ต้องปิดทำการและกลับมาใช้การขนส่งสำรอง ซึ่งหากแฮกเกอร์ (Hacker) มุ่งทำลายระบบการขนส่งน้ำมันอาจทำให้เกิดอันตรายต่อชีวิตพนักงานของบริษัท Colonial Pipeline และประชาชนบริเวณโดยรอบได้

ประเทศไทยก็ได้รับผลกระทบโดยตรงต่อภัยคุกคามทางไซเบอร์ โรงพยาบาลสระบุรีได้ตกเป็นเป้าหมายของการโจรกรรมข้อมูลด้วยโปรแกรมประสงค์ร้ายเรียกค่าไถ่[๑] ทำให้แพทย์และพยาบาลทำงานล่าช้าลงเนื่องจากไม่สามารถเข้าถึงข้อมูลผู้ป่วยได้ โดยทางโรงพยาบาลสระบุรีได้ออกมาประกาศผู้ใช้บริการโรงพยาบาลทุกคนทราบว่า ระบบคอมพิวเตอร์ของโรงพยาบาลกำลังถูกเข้ารหัสข้อมูลทำให้ไม่สามารถเข้าถึงข้อมูลผู้ป่วยที่อยู่ในเซิร์ฟเวอร์ได้ ซึ่งข้อมูลซึ่งถูกเข้ารหัสนั้นล้วนเป็นข้อมูลผู้ป่วยในระบบซึ่งเป็นข้อมูลที่จำเป็นต่อการรักษาและวินิจฉัยโรคเป็นอย่างมาก ซึ่งในเหตุการณ์นี้อาจทำให้มีผู้เสียชีวิตได้เนื่องจากความล่าช้าในการรักษา ในกองทัพอากาศ ศูนย์ข้อมูลคอมพิวเตอร์ สอ.ทอ.ถูกแฮกเกอร์โจมตีระบบฐานข้อมูลควบคุมบริหารจัดการบัญชี ทำให้ข้อมูล Username/Password ทอ.รั่วไหล[๒] และถูกเรียกค่าไถ่ ส่งผลกระทบต่อการปฏิบัติงานด้วยระบบเทคโนโลยีสารสนเทศของกองทัพอากาศ

จากเหตุการณ์ข้างต้นแสดงให้เห็นว่า ภัยคุกคามทางไซเบอร์มีความรุนแรงในทุกระดับ ดังนั้นเพื่อเป็นการรับมือกับภัยคุกคามทางไซเบอร์ กระทรวงกลาโหมจึงได้อนุมัติให้จัดตั้งศูนย์ไซเบอร์ขึ้นในทุกเหล่าทัพ ในส่วนกองทัพอากาศ ได้ตระหนักถึงความจำเป็นในการหาวิธีการป้องกันและรับมือกับภัยคุกคามดังกล่าวอย่างเป็นรูปธรรมจึงได้จัดตั้งศูนย์ไซเบอร์กองทัพอากาศขึ้นเมื่อปี พ.ศ.๒๕๖๓ และยุทธศาสตร์ ๒๐ ปี มุ่งพัฒนาขีดความสามารถด้านการปฏิบัติการไซเบอร์ของกองทัพอากาศ ผ่านการ

---

[๑] (๑๐ ก.ย. ๒๕๖๓) “แฮ็กโรงพยาบาล-รีดค่าไถ่ เรียกถึง ๖.๓ หมื่นล้านบาท”, สืบค้นเมื่อ ๒๕๖๕ https://www.thairath.co.th/news/local/central/1926912

[๒] “สรุปผลการตรวจสอบเหตุการณ์ข้อมูล Username/Password ทอ.รั่วไหล”ก.ค.๒๕๖๓.

พัฒนาเทคโนโลยี โครงสร้างพื้นฐาน โครงสร้างองค์กร บุคลากร และองค์ความรู้ เพื่อป้องกันภัยคุกคามทางไซเบอร์ ตามมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือ (Cyber Security)[๓] รวมทั้งการเตรียมความพร้อมในการปฏิบัติการเชิงรุก และแสวงหาความร่วมมือกับหน่วยงานทั้งภายในและภายนอกประเทศ เช่น การประชุมประชาคมไซเบอร์ การฝึกการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่วนภายนอกประเทศ เช่น การประชุมผู้เชี่ยวชาญทางไซเบอร์ระหว่างไทย-สหรัฐอเมริกา และมิตรประเทศรอบบ้าน เพื่อแลกเปลี่ยนองค์ความรู้ไซเบอร์ เพื่อนำมาประยุกต์ใช้ในการป้องกันภัยคุกคามทางไซเบอร์ การรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งหากถูกโจมตีทางไซเบอร์ต่อระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ ก็สามารถรับมือกับภัยคุกคามไซเบอร์ตามแนวทางการพัฒนาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ และสามารถกู้คืนระบบและฟื้นตัวให้สามารถกลับมาใช้งานตามปกติได้อย่างรวดเร็ว

กองทัพอากาศได้นำการปฏิบัติการไซเบอร์[๔]มาปรับใช้เป็นหลักนิยมการปฏิบัติการไซเบอร์ของกองทัพอากาศ หรือ (Cyber Conops) ซึ่งประกอบด้วย การปฏิบัติการข่าวกรองไซเบอร์ การปฏิบัติการไซเบอร์เชิงป้องปราม การปฏิบัติการไซเบอร์เชิงป้องกัน[๕] กล่าวคือ การปฏิบัติการข่าวกรองไซเบอร์มีเป้าหมายเพื่อ วางแผน รวบรวม วิเคราะห์ ข่าวกรองเพื่อสนับสนุนการปฏิบัติการทั้งเชิงรุกและเชิงรับ เพื่อให้ประสบความสำเร็จในการปฏิบัติการไซเบอร์ ซึ่งมีหลักการมาจากงานข่าวกรองในปฏิบัติการทางทหารมักใช้เทคโนโลยีด้านการข่าวที่มีมิติไซเบอร์เป็นสื่อกลางในการค้นหารวบรวม ดักฟัง ขโมยข้อมูลของฝ่ายตรงข้าม เพื่อช่วงชิงความได้เปรียบในเรื่องข้อมูลข่าวสารเพื่อประกอบการตัดสินใจของผู้บังคับบัญชา โดยมุ่งพัฒนาระบบรวบรวมข้อมูลด้านการปฏิบัติการลาดตระเวนในมิติไซเบอร์ของข้าศึกเพื่อจัดทำบัญชีเป้าหมายทางไซเบอร์

งานข่าวกรองไซเบอร์ (Cyber Intelligence)[๖] มีการปฏิบัติเช่นเดียวกับงานข่าวกรองในมิติอื่นๆ โดยมีรูปแบบและวงรอบข่าวกรองทางไซเบอร์ซึ่งประกอบด้วย การอำนวยการ การรวบรวม การประมวลผล การวิเคราะห์ การเผยแพร่ใช้ประโยชน์ และการเสนอแนะ ซึ่งหน้าที่และขีดความสามารถที่จำเป็นของข่าวกรองไซเบอร์ คือ การระบุถึงภัยคุกคามและหนทางปฏิบัติของฝ่ายตรงข้าม การจัดทำฐานข้อมูลทางด้านความมั่นคงปลอดภัยไซเบอร์ การเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ การจัดทำเป้าหมายทางไซเบอร์เพื่อสนับสนุนการปฏิบัติการไซเบอร์เชิงป้องปราม และการเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์หรือ (Intelligence Preparation of the Cyber Environment: IPCE) ตัวอย่าง การดำเนินงานที่ผ่านมา คือการจัดทำแฟ้มบัญชีเป้าหมายทางไซเบอร์เพื่อสนับสนุนข้อมูลในทำเนียบกำลังรบของประเทศตรงข้าม

ในปัจจุบัน หน่วยงานด้านความมั่นคงของรัฐมีการประยุกต์ใช้งานระบบข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence: CTI) จากหลายแหล่ง (Sources) เพื่อใช้ในการตรวจสอบภัยคุกคามไซเบอร์ โดยข้อมูลข่าวกรองดังกล่าวประกอบด้วย ฐานข้อมูลเว็บไซต์ ยูอาร์แอล ข้อมูลมัลแวร์

---

[๓] “Cyber Security”. Accessed 2021, https://www.rdpb.go.th/MediaUploader/File/10166/CyberSecurity

[๔] SCOTT JASPER. (2020) “RUSSIAN CYBER OPERATIONS”

[๕] “หลักนิยมการปฏิบัติการไซเบอร์” ๒๕๖๓.

[๖] (2013). “Joint Publication 2-0 joint intelligence”. Accessed 2021, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf

หมายเลขไอพีอันตรายที่ผ่านการตรวจสอบแล้วว่าเป็นกลุ่มไอพีที่ถูกแฮกเกอร์ใช้เป็นเครื่องมือในการโจมตีหรือสร้างความเสียหายให้กับระบบเครือข่ายคอมพิวเตอร์ และข้อมูลการโจมตีเหล่านี้มีการเผยแพร่สู่สาธารณะตามแหล่งข้อมูลที่เรียกกันว่า Blacklist IP หรือข้อมูลช่องโหว่ (Vulnerability) ซึ่งถือว่าเป็นข้อมูลสำคัญที่สามารถใช้ในการบ่งชี้ว่าระบบดังกล่าวถูกโจมตีหรือถูกบุกรุก (Indicator of Compromises: IOCs) โดยฐานข้อมูลเหล่านี้ สามารถนำมาปรับปรุงพัฒนา การเฝ้าระวัง ตรวจจับ แจ้งเตือน และวิเคราะห์ภัยคุกคามทางไซเบอร์ เพื่อให้หน่วยงานสามารถรับมือกับภัยคุกคามเหล่านั้นได้อย่างทันท่วงทีเพื่อป้องกันไม่ให้เกิดความเสียหายต่อหน่วยงาน ดังนั้นจึงจำเป็นอย่างยิ่งที่ต้องมีกระบวนการตรวจสอบข้อมูลภัยคุกคามจากหลายแหล่งที่มา เพื่อเพิ่มความน่าเชื่อถือของข้อมูลที่ถูกนำไปใช้ในการนำไปวิเคราะห์และเฝ้าระวังการโจมตีจากภัยคุกคามทางไซเบอร์

จากความสำคัญของปัญหาที่กล่าวมาข้างต้น ผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงนักวิจัยจึงได้พัฒนาแนวความคิดในการรวบรวมข้อมูลภัยคุกคามไซเบอร์โดยอัตโนมัติ เพื่อรวบรวมข้อมูลหมายเลขไอพี ชื่อโดเมน ยูอาร์แอล ที่เป็นภัย คุกคาม รวมถึงข้อมูล IOCs จากหลายแหล่ง เพื่อเข้ามาช่วยในการวิเคราะห์ เฝ้าระวัง ตรวจจับ แจ้งเตือนการโจมตีของภัยคุกคาม ทำให้สามารถประเมินเหตุการณ์ สามารถคาดคะเน รวมถึงประเมินสถานการณ์เกี่ยวกับภัยคุกคามที่หน่วยงานกำลังเผชิญอยู่ รวมถึงการสืบสวนหาบุคคลผู้อยู่เบื้องหลัง วัตถุประสงค์ แรงจูงใจ และเป้าหมายในการคุกคามต่อระบบ รวมถึงวิเคราะห์ระบบภายในหน่วยงานที่อาจเป็นเป้าหมายที่ถูกโจมตีด้วยเหตุนี้ผู้วิจัยจึงมีความสนใจที่จะศึกษาวิจัย เรื่อง “ศึกษาและทดสอบ Cyber Threat Intelligence Feeds หลายแหล่งเพื่อปรับใช้กับระบบข่าวกรองภัยคุกคามทางไซเบอร์แบบไม่เสียค่าใช้จ่าย” เพื่อศึกษาวิเคราะห์ หาแนวทางพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ ที่สมควรจะต้องได้รับการพัฒนาอย่างเป็นรูปธรรม ซึ่งการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันภัยคุกคามที่จะเกิดขึ้นได้อย่างมีประสิทธิภาพและประสบความสำเร็จนั้น จำเป็นอย่างยิ่งที่จะต้องมีงานข่าวกรองไซเบอร์ที่เข้มแข็ง ซึ่งถือเป็นความท้าทายใหม่ของกองทัพอากาศ ที่ยังขาดบุคลากรและองค์ความรู้ ในการพัฒนาข่าวกรองไซเบอร์ในระดับกลาโหม ผู้วิจัยจึงมีความสนใจในการศึกษาวิจัยเพื่อจัดทำ “แนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ” เพื่อให้หน่วยงานและบุคคลที่เกี่ยวข้อง สามารถนำไปใช้ประโยชน์ต่อไป

๒. วัตถุประสงค์การวิจัย

๒.๑ เพื่อศึกษาแนวทางการใช้ประโยชน์จากข่าวกรองภัยคุกคามทางไซเบอร์ที่มีความเหมาะสมต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ

๒.๒ เพื่อพัฒนาต้นแบบและทดสอบการใช้งานข่าวกรองภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพด้วยวิธีการบูรณาการชุดข้อมูลจากหลากหลายแหล่งที่มา

๒.๓ เพื่อเสนอแนะแนวทางในการใช้ประโยชน์จากต้นแบบการใช้งานข่าวกรองภัยคุกคามทางไซเบอร์ด้วยวิธีบูรณาการชุดข้อมูลจากหลากหลายแหล่งที่มาให้แก่หน่วยงานที่เกี่ยวข้องในกองทัพอากาศ

๓. คำถามการวิจัย

๓.๑ แนวทางในการใช้ประโยชน์จากข่าวกรองภัยคุกคามทางไซเบอร์อย่างไรที่มีความเหมาะสมต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศเป็นอย่างไร

๓.๒ วิธีการพัฒนาต้นแบบด้านงานข่าวกรองภัยคุกคามทางไซเบอร์จากการบูรณาการข้อมูลจากหลายแหล่งที่มาที่มีประสิทธิภาพต้องมีขั้นตอนในการดำเนินการอย่างไรและมีวิธีการวัดผลลัพธ์อย่างไร

๓.๓ กองทัพอากาศควรมีแนวทางในการใช้ประโยชน์จากต้นแบบการใช้งานข่าวกรองภัยคุกคามทางไซเบอร์ด้วยวิธีบูรณาการชุดข้อมูลจากหลากหลายแหล่งที่มารวมถึงการขยายผลไปยังหน่วยงานที่เกี่ยวข้องในกองทัพอากาศอย่างไร

๔. ขอบเขตของการวิจัย

๔.๑ ระบบสามารถดึงข้อมูลภัยคุกคามทางไซเบอร์แบบอัตโนมัติจากแหล่งข้อมูลต่าง ๆ ในการวิเคราะห์ตรวจจับภัยคุกคามที่เข้ามายังระบบข่าวกรองภัยคุกคามทางไซเบอร์แบบไม่เสียค่าใช้จ่าย

๔.๒ ระบบสามารถทำการเชื่อมต่อกับผู้ให้บริการ Cyber Threat Intelligence Analyzer เช่น AlienVault, MITRE, CVE, TAXII2

๔.๓ ระบบสามารถรายงานผลการตรวจสอบ Cyber Threat Intelligence Analyzer

๕. วิธีการวิจัย

๕.๑ ศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้อง

๕.๒ ศึกษาเทคนิค Cyber Threat Intelligence Feeds

๕.๓ ดำเนินการพัฒนาระบบ Cyber Threat Intelligence Feeds

๕.๔ ทดสอบระบบ Cyber Threat Intelligence Feeds ครั้งที่ ๑

๕.๕ พัฒนาและปรับปรุงระบบ Cyber Threat Intelligence Feeds

๕.๖ ทดสอบระบบ Cyber Threat Intelligence Feeds ครั้งที่ ๒ และประเมินผล

๕.๗ ทำการปรับปรุงระบบ Cyber Threat Intelligence Feeds ให้พร้อมใช้งาน

๕.๘ ทำการสรุปผลการวิจัย

๕.๙ จัดทำเอกสารวิจัย

๖. ประโยชน์ที่คาดว่าจะได้รับ

๖.๑. ลดความซ้ำซ้อนของข้อมูลภัยคุกคามไซเบอร์โดยอัตโนมัติเป็นกระบวนการสำคัญในการรับข้อมูลจากหลายแหล่งที่มา

๖.๒ ลดข้อมูลไร้ประโยชน์จำนวนมากซึ่งส่งผลกระทบต่อการคัดแยก ประมวลผล และดำเนินการ เพื่อปรับใช้กับระบบข่าวกรองภัยคุกคามทางไซเบอร์

๖.๓ มีกระบวนการในการตรวจสอบความถูกต้องของข้อมูลข่าวกรองที่ได้มา

๖.๔ ลดปัญหาด้านความล่าช้าของการส่งข้อมูลภัยคุกคามหลังจากตรวจจับได้ เข้าสู่ระบบข่าวกรองภัยคุกคามทางไซเบอร์

๖.๕ ลดภาระค่าใช้จ่ายด้านงบประมาณในการจัดหาข่าวกรองทางไซเบอร์จากแหล่งข้อมูลที่มีค่าบริการทางข้อมูล รวมถึงส่งเสริมการพึ่งพาตนเองได้ขององค์กร

๖.๖ กองทัพอากาศสามารถรับมือกับภัยคุกคามทางไซเบอร์ในอนาคต

๗. คำนิยามศัพท์เฉพาะ

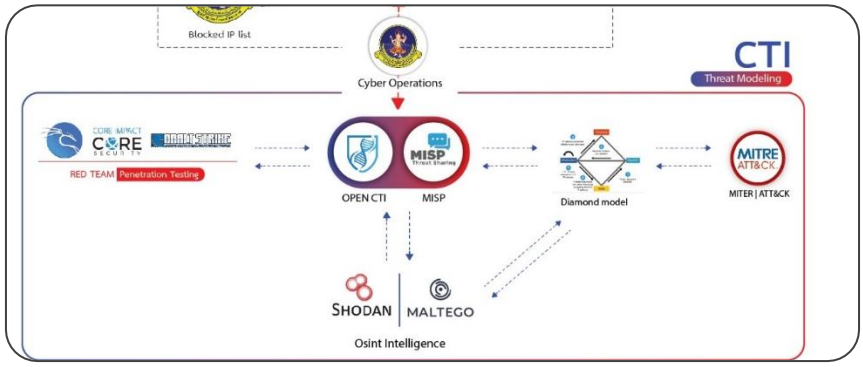
ไซเบอร์ หมายถึง กิจกรรมที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ การสื่อสารข้อมูลคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์

ความมั่นคงปลอดภัยไซเบอร์ หมายถึง มาตรการและการดำเนินการเพื่อปกป้องป้องกันการส่งเสริม เพื่อรับมือและแก้ไขสถานการณ์ด้านภัยคุกคามที่จะส่งผลต่อไซเบอร์ โดยเฉพาะการให้บริการด้านระบบเครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม การให้บริการดาวเทียม ระบบกิจการสาธารณูปโภคพื้นฐาน ระบบกิจการสาธารณะสำคัญ ซึ่งเป็นเครือข่ายในระดับประเทศ เพื่อมิให้เกิดผลกระทบต่อความมั่นคงของชาติ ความมั่นคงทางการทหาร ความสงบเรียบร้อย ภายในประเทศ และความมั่นคงทางเศรษฐกิจ

ภัยคุกคามทางไซเบอร์ หมายความว่า หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

๘. กรอบแนวคิดงานวิจัย

งานวิจัยนี้มุ่งเน้นพัฒนาระบบการรวบรวมข่าวกรองทางไซเบอร์ผ่านการดึงข้อมูลภัยคุกคามทางไซเบอร์ผ่านแหล่งข่าวกรองทางไซเบอร์ต่าง ๆ และนำมาประมวลผลข่าวกรองทางไซเบอร์ที่น่าเชื่อถือ จากนั้นส่งต่อข้อมูลข่าวกรองดังกล่าวไปยังหน่วยงานที่เกี่ยวข้อง พร้อมจัดทำรายงานผลการตรวจสอบ ดังแสดงในภาพที่ ๑.๑

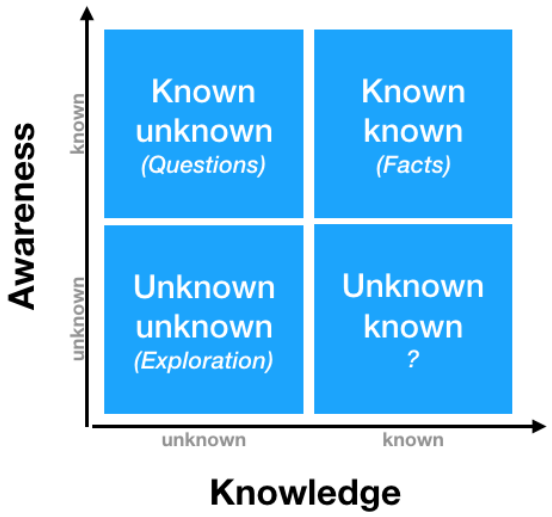


ภาพที่ ๑.๑ กรอบแนวคิดงานวิจัย

บทที่ ๒
การทบทวนวรรณกรรม

๒.๑ ข่าวกรองทางไซเบอร์

การข่าวกรอง (Intelligence) เป็นงานที่เกี่ยวข้องโดยตรงกับความมั่นคงปลอดภัยผ่านการสืบราชการลับ การหาข่าวกรอง เช่น Human Intelligence (HUMINT) กล่าวคือ การใช้คนในการลงพื้นที่เพื่อหาข่าว Signal Intelligence (SIGINT) หรือการใช้อุปกรณ์ดักฟังการสื่อสาร การตัดการสื่อสาร การแปลงข่าวสารให้ มีข้อความที่เปลี่ยนไปซึ่ง SIGINT ยังแบ่งย่อยออกได้เป็น ๒ ชนิด คือ COMINT และ ELINT โดยมิติไซเบอร์จะเรียกการข่าวกรองที่แสวงหาได้จากมิติทางไซเบอร์ว่า Cyber Intelligence (CYBERINT) ด้วยการพัฒนาอย่างรวดเร็วทางด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงความง่ายต่อการเข้าถึงโลกไซเบอร์มากขึ้น ข้อมูลที่ถูกส่งผ่านการสื่อสารในโลกไซเบอร์เพิ่มมากขึ้นตามลำดับทั้งบนดินและใต้ดิน (ทองม่วง, ๒๕๖๓) (Perkins, 2023)



ภาพที่ ๒.๑ การเปลี่ยนแปลงของผลลัพธ์ในข่าวกรอง[๗]

ข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence: CTI) มีที่มาจากการทำข่าวกรองภัยคุกคาม (Threat Intelligence) ซึ่งเกี่ยวข้องกับข้อมูลภัยคุกคามที่นำเข้ามาเพื่อพิสูจน์และประกอบการพิจารณาตัดสินใจ เพื่อหา แนวทางในการป้องกันผู้บุกรุก หรือป้องกันการโจมตีระบบขององค์กร (พงษ์ศักดิ์, ๒๕๖๑) ในรายงานของ Centre for the Protection of National

[๗] The Persimmon Group. (n.d.). How to use the "Knowns" and "Unknowns" technique to manage assumptions. The Persimmon Group. Retrieved December 2, 2024, from https://thepersimmongroup.com/how-to-use-the-knowns-and-unknowns-technique-to-manage-assumptions/

Infrastructure (CPNI) และ MWR InfoSecurity (2015) ได้ให้คำนิยามเกี่ยวกับข่าวกรองภัยคุกคามทางไซเบอร์ว่าเป็นข้อมูลภัยคุกคามที่นำไปใช้แล้วเกิดการเปลี่ยนแปลงของผลลัพธ์ (CPNI & MWR InfoSecurity, 2015) ยกตัวอย่าง เช่น การบันทึกใช้สิ่งที “รู้” (Knowns) และ “ไม่รู้” (Unknowns) ภายในข้อมูลข่าวกรอง (Intelligence) ที่รวบรวมได้ กรณีที่มีข้อมูลข่าวกรองน้อยก็จะมีปัญหาเรื่อง “ไม่รู้” “ไม่รู้” (Unknowns Unknowns) เมื่อไม่มีข่าวกรองเราก็จะไม่รู้ ว่าเรา “ไม่รู้” ว่าเรา “ไม่รู้” อะไรบ้าง เมื่อมีข่าวกรองเราก็จะเริ่ม “รู้” ว่าเรายัง “ไม่รู้” เรื่อง อะไรบ้าง (Known Unknowns) และเมื่อมีเรามีข้อมูลในข่าวกรองภัยคุกคามทางไซเบอร์อย่างเพียงพอ ย่อส่งผลต่อการเปลี่ยนการโจมตีจาก “Unknowns Unknowns” ให้กลายเป็น “Knowns Knowns” ดังแสดงในภาพที่ ๒.๑

การค้นหาการข่าวกรองทางไซเบอร์ (Cyber Intelligence: CYBERINT) ในปัจจุบันมีการพัฒนาเครื่องมือในการรวบรวมข้อมูลข่าวกรองโดยนำเอา OSINT (Opensource Intelligence) มาใช้เพื่อกวาดข้อมูลในโลกออนไลน์จากแหล่งข้อมูลเปิดทั้งหลาย เช่น เว็บไซต์ เว็บบอร์ด เครือข่ายสังคมออนไลน์ ที่เปิดไว้เป็นสาธารณะ แล้วนำมาประมวลผลเพื่อประโยชน์ในการทำเฝ้าระวังทางธุรกิจในด้านของ Cybersecurity ก็เช่นกัน (Central Intelligence Agency, 2023) หนึ่งใน ปัจจัยของความสำเร็จของศูนย์ SOC คือ Cyber Threat Intelligence (SOC CTI) เป็นการรวบรวม ข้อมูลภัยคุกคามจากหลายแหล่ง เข้ามาแล้วทำการคัดแยก ประมวลผล และดำเนินการเพื่อสร้าง Cyber Threat Intelligence ขึ้นมา และนำข้อมูลที่ได้ไปตรวจสอบกับผู้ให้บริการ Cyber Threat Intelligence Analyzer เพื่อทำการวิเคราะห์ว่าขณะนี้องค์กรกำลังเผชิญหน้ากับอะไร ผู้ที่อยู่เบื้องหลังคือใคร ต้องการทำอะไรกับระบบ เป้าหมายของการโจมตีคือระบบไหนในองค์กร รวมไปถึงพฤติกรรมเชิงลึกของภัยคุกคามร่วมกับฐานข้อมูลของการโจมตีที่รู้จัก ช่วยให้องค์กรสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที Cyber Threat Intelligence ที่ดีนั้น ช่วยให้สามารถคาดการณ์การโจมตีล่วงหน้าได้ก่อนที่เหตุการณ์จะเกิดขึ้น

การปฏิบัติการข่าวกรองการเฝ้าตรวจและลาดตระเวนทางไซเบอร์ (Cyber Intelligence, Surveillance and Reconnaissance: Cyber ISR) คือ การปฏิบัติการเพื่อให้ได้มาซึ่งข้อมูลข่าวสารผ่านเครือข่ายคอมพิวเตอร์ ด้วยการค้นหารวบรวมข้อมูลจากระบบเป้าหมายหรือเครือข่ายและระบบของฝ่ายตรงข้าม นำมาซึ่งข้อมูลข่าวกรองและการสร้างความตระหนักรู้สถานการณ์ (Situation Awareness: SA) เพื่อการตัดสินตกลงใจของผู้บังคับบัญชาดังแสดงในภาพ ๒.๒ ประกอบด้วยขั้นตอนสำคัญที่ช่วยในการรวบรวม วิเคราะห์ และเผยแพร่ข้อมูลภัยคุกคามไซเบอร์อย่างมีประสิทธิภาพ ภาพด้านบนแสดงถึงองค์ประกอบหลักของวงจรนี้ ซึ่งประกอบด้วย ๑) การวางแผนและกำกับ (Planning and Directing): กำหนดวัตถุประสงค์และขอบเขตของการรวบรวมข้อมูลภัยคุกคาม, ๒) การสะสม (Collection): รวบรวมข้อมูลจากแหล่งต่าง ๆ เช่น โซเชียลมีเดีย เว็บบอร์ด และฐานข้อมูล, ๓) การประมวลผลและใช้ประโยชน์ (Processing and Exploration): จัดระเบียบและกรองข้อมูลที่รวบรวมมาเพื่อเตรียมสำหรับการวิเคราะห์, ๔) การวิเคราะห์และการผลิต (Analysis and Production): วิเคราะห์ข้อมูลเพื่อสร้างรายงานหรือข้อมูลเชิงลึกเกี่ยวกับภัยคุกคาม, ๕) การเผยแพร่และบูรณาการ (Integration): ส่งต่อข้อมูลที่วิเคราะห์แล้วไปยังผู้ที่เกี่ยวข้องหรือหน่วยงานที่ต้องการ จากนั้นจึงทำการวิเคราะห์การตอบสนองและการดำเนินการ (Feedback and Action) เพื่อรับข้อมูลย้อนกลับและดำเนินการตามข้อมูลที่ได้รับเพื่อปรับปรุงกระบวนการ การทำความเข้าใจและ

ปฏิบัติตามวงจรนี้ช่วยให้องค์กรสามารถจัดการกับภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพ (National Cyber Security Centre, 2014)

ภาพที่ ๒.๒ วงจรการปฏิบัติการข่าวกรองการเฝ้าตรวจและลาดตระเวนทางไซเบอร์

๒.๒ ข่าวกรองภัยคุกคามทางไซเบอร์

ข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence) คือกระบวนการรวบรวม วิเคราะห์ และตีความข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อองค์กรหรือระบบสารสนเทศ ซึ่งข้อมูลเหล่านี้ช่วยให้องค์กรเข้าใจถึงแหล่งที่มาของภัยคุกคาม วิธีการโจมตี และเป้าหมายที่ผู้ไม่หวังดีมุ่งเน้น โดยเป็นประโยชน์ในการวางแผนป้องกันและตอบสนองต่อเหตุการณ์ทางไซเบอร์อย่างมีประสิทธิภาพ (Microsoft, n.d.)

การใช้ข่าวกรองภัยคุกคามทางไซเบอร์มีความสำคัญอย่างยิ่งในยุคที่เทคโนโลยีสารสนเทศเข้ามามีบทบาทในทุกภาคส่วน โดยเฉพาะอย่างยิ่งเมื่อภัยคุกคามมีความซับซ้อนและพัฒนาอย่างต่อเนื่อง การมีข้อมูลที่ถูกต้องและทันเวลาเกี่ยวกับภัยคุกคามจะช่วยให้องค์กรสามารถตัดสินใจและดำเนินการป้องกันได้อย่างเหมาะสม เช่น การปรับปรุงระบบรักษาความปลอดภัย การฝึกอบรมพนักงาน และการวางแผนตอบสนองต่อเหตุการณ์ (SANS Institute, 2022)

นอกจากนี้ ข่าวกรองภัยคุกคามทางไซเบอร์ยังช่วยให้องค์กรสามารถระบุและจัดลำดับความสำคัญของความเสี่ยงที่อาจเกิดขึ้น รวมถึงการตรวจสอบและประเมินช่องโหว่ในระบบ เพื่อป้องกันการโจมตีที่อาจเกิดขึ้นในอนาคต การมีความเข้าใจที่ชัดเจนเกี่ยวกับภัยคุกคามจะช่วยให้องค์กรสามารถวางกลยุทธ์การป้องกันที่มีประสิทธิภาพและลดความเสี่ยงที่อาจเกิดขึ้นได้ (สำนักข่าว

กรองแห่งชาติ, n.d.) สำหรับประเภทของข่าวกรองภัยคุกคามทางไซเบอร์แบ่งออกเป็น ๔ ประเภท ประกอบด้วย

๒.๒.๑ ข่าวกรองเชิงกลยุทธ์ (Strategic Threat Intelligence) เป็นข้อมูลที่เน้นการให้ภาพรวมเกี่ยวกับแนวโน้มและเป้าหมายระยะยาวของภัยคุกคามทางไซเบอร์ รวมถึงการวิเคราะห์ภาพรวมของสถานการณ์เพื่อสนับสนุนการตัดสินใจเชิงกลยุทธ์ โดยมักใช้โดยผู้บริหารระดับสูงเพื่อกำหนดทิศทางและแผนการดำเนินงานขององค์กร (Microsoft, n.d.)

๒.๒.๒ ข่าวกรองเชิงปฏิบัติการ (Operational Threat Intelligence) เป็นข้อมูลที่เกี่ยวข้องกับแผนการหรือกิจกรรมเฉพาะของผู้โจมตี เช่น แคมเปญการโจมตีที่กำลังดำเนินอยู่ หรือเครื่องมือที่ใช้ในการโจมตี โดยข่าวกรองลักษณะนี้ช่วยให้หน่วยงานด้านความปลอดภัยเข้าใจรูปแบบและเป้าหมายการโจมตีเพื่อเตรียมการตอบสนองได้อย่างเหมาะสม (SANS Institute, 2022)

๒.๒.๓ ข่าวกรองเชิงเทคนิค (Technical Threat Intelligence) เป็นข้อมูลที่เกี่ยวข้องกับรายละเอียดทางเทคนิค เช่น มัลแวร์ ตัวบ่งชี้ของการบุกรุก (Indicators of Compromise: IoCs) และข้อมูลเกี่ยวกับระบบที่ตกเป็นเป้าหมาย โดยมักใช้ในกระบวนการตรวจจับและป้องกันภัยคุกคามในระดับระบบ (สำนักข่าวกรองแห่งชาติ, n.d.)

๒.๒.๔ ข่าวกรองเชิงยุทธวิธี (Tactical Threat Intelligence) เป็นข้อมูลที่มุ่งเน้นการวิเคราะห์วิธีการ เทคนิค และขั้นตอน (Tactics, Techniques, and Procedures: TTPs) ของผู้โจมตี เพื่อช่วยในการวางแผนป้องกันและกำหนดมาตรการรักษาความปลอดภัยในระดับปฏิบัติการ เช่น การออกแบบระบบที่สามารถรับมือกับการโจมตีรูปแบบต่าง ๆ ได้ (Microsoft, n.d.)

๒.๓ ความท้าทายในการหาข่าวกรองทางไซเบอร์

ในปัจจุบัน ด้วยความก้าวหน้าทางเทคโนโลยีการติดต่อสื่อสารทางอินเทอร์เน็ต รวมถึงระบบอินเทอร์เน็ตของสรรพสิ่ง (Internet of Things: IoTs) ทำให้เกิดการไหลเวียนของข้อมูลสารสนเทศบนระบบเครือข่ายคอมพิวเตอร์อย่างมหาศาล ส่งให้ผลให้เกิดความท้าทายในด้านข้อมูลในการหาข่าวกรองทางไซเบอร์ โดยความท้าทายดังกล่าวประกอบด้วย

๒.๓.๑ ปริมาณข้อมูลมหาศาล (Volume)

ในโลกดิจิทัลที่มีการสร้างข้อมูลอย่างต่อเนื่อง ปริมาณข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ก็เพิ่มขึ้นอย่างมหาศาลในแต่ละวัน ไม่ว่าจะเป็นข้อมูลจากอุปกรณ์ IoT, โซเชียลมีเดีย, หรือระบบเครือข่ายขององค์กร ปริมาณข้อมูลที่มากเกินไปทำให้การจัดเก็บ การวิเคราะห์ และการค้นหาข้อมูลที่มีค่าต้องใช้ระบบประมวลผลที่มีประสิทธิภาพ เช่น ระบบจัดการข้อมูลแบบกระจาย (Distributed Systems) หรือคลังข้อมูลขนาดใหญ่ รวมถึงความท้าทายต่อข้อมูลที่อาจมีความซ้ำซ้อน (Marr, 2020)

๒.๓.๒ การตรวจสอบความถูกต้อง (Veracity)

ข้อมูลจำนวนมากที่รวบรวมได้อาจไม่ถูกต้องหรือไม่สมบูรณ์ การตรวจสอบความถูกต้องของข้อมูลจึงเป็นเรื่องที่ท้าทาย โดยเฉพาะในกรณีที่มีข้อมูลเท็จ (False Data) หรือข้อมูลที่สร้างขึ้นเพื่อบิดเบือนข้อเท็จจริง รวมถึงการคัดกรองข้อมูลที่แฮกเกอร์ปล่อยมาเพื่อให้สร้างข่าวกรอง

เท็จในแบบที่แฮกเกอร์ต้องการ การกรองและยืนยันข้อมูลที่เชื่อถือได้ต้องใช้ทั้งเครื่องมือที่ทันสมัยและบุคลากรที่มีความเชี่ยวชาญ (Microsoft, n.d.)

๒.๓.๓ คุณภาพของข้อมูล (Quality)

ไม่ใช่ทุกข้อมูลที่ถูกรวบรวมมาจะมีคุณภาพสูงหรือเหมาะสมสำหรับการใช้งาน ข่าวกรองภัยคุกคามที่ได้จากแหล่งต่าง ๆ อาจมีความแตกต่างในรูปแบบ โครงสร้าง หรือความสมบูรณ์ ซึ่งการทำให้ข้อมูลทั้งหมดเป็นมาตรฐานเดียวกันเพื่อใช้ในการวิเคราะห์เป็นเรื่องที่ต้องใช้ทรัพยากรและเวลาอย่างมาก (Marr, 2020) ดังนั้น การกรอง แท็ก และการขจัดความซ้ำซ้อนของข้อมูลโดยอัตโนมัติจึงถือเป็นกระบวนการสำคัญในการรับข้อมูลจากหลายแหล่งที่มา

๒.๓.๔ ความรวดเร็วในการวิเคราะห์ (Velocity)

การตอบสนองต่อภัยคุกคามทางไซเบอร์ต้องการข้อมูลที่ทันเวลาและรวดเร็ว ความล่าช้าในการวิเคราะห์ข้อมูลอาจทำให้องค์กรไม่สามารถป้องกันหรือตอบสนองต่อการโจมตีได้ทัน เช่น การป้องกันมัลแวร์หรือการแก้ไขช่องโหว่ในระบบ การแลกเปลี่ยนข้อมูลแบบเปิดที่ได้มาตรฐานช่วยขจัดปัญหาด้านความล่าช้าของการส่งข้อมูลภัยคุกคามหลังจากตรวจจับได้ และส่งข้อมูลเข้าสู่ระบบข่าวกรองทางไซเบอร์ รวมถึงการใช้เทคโนโลยี Real-time Analytics และ AI ช่วยในการวิเคราะห์ข้อมูลจึงมีความสำคัญอย่างยิ่ง (Microsoft, n.d.)

๒.๓.๕ การทำความเข้าใจความสัมพันธ์ของข้อมูล (Correlation)

ภัยคุกคามทางไซเบอร์มักมีลักษณะซับซ้อนและเกี่ยวข้องกับหลายปัจจัย การเชื่อมโยงข้อมูลจากหลายแหล่ง เช่น ความสัมพันธ์ระหว่างระบบปฏิบัติการ อุปกรณ์ และระบบเครือข่าย เพื่อระบุความสัมพันธ์ระหว่างเหตุการณ์หรือพฤติกรรมที่อาจเป็นอันตรายและกำหนดขอบเขตการดำเนินการเพื่อตอบสนองเป็นเรื่องที่ท้าทาย ตัวอย่างเช่น การเชื่อมโยงพฤติกรรมของผู้ใช้ที่ผิดปกติกับการโจมตีในลักษณะฟิชชิ่ง (Phishing) การทำความเข้าใจความสัมพันธ์ที่ซับซ้อนเหล่านี้จำเป็นต้องใช้เครื่องมือวิเคราะห์ข้อมูลขั้นสูง เช่น Machine Learning หรือ Graph Analytics (Marr, 2020; Microsoft, n.d.)

๒.๔ Indicator of Compromise

Indicator of Compromise (IoC) ในความมั่นคงปลอดภัยไซเบอร์ คือหลักฐานหรือข้อมูลที่สามารถใช้ระบุถึงการมีอยู่ของภัยคุกคามทางไซเบอร์ในระบบหรือเครือข่ายขององค์กร IoC เป็นสิ่งที่บ่งชี้ว่าระบบอาจถูกโจมตีหรือได้รับผลกระทบจากการดำเนินการที่ไม่พึงประสงค์ เช่น การติดมัลแวร์ การเข้าถึงโดยไม่ได้รับอนุญาต หรือการละเมิดข้อมูล (Symantec, n.d.) (SANS Institute, 2019) (Kaspersky, n.d.) โดย IoC อาจมาจากหลายแหล่งที่มา เช่น

๑) ที่อยู่ IP ที่น่าสงสัย เช่น ที่อยู่ IP ที่เป็นที่รู้จักว่าเกี่ยวข้องกับกิจกรรมอันตราย เช่น การโจมตีแบบ Distributed Denial of Service (DDoS) หรือเซิร์ฟเวอร์ C&C (Command and Control)

๒) ชื่อโดเมนหรือ URL ที่ไม่ปลอดภัย ลิงก์หรือชื่อโดเมนที่ใช้ส่งฟิชชิ่งอีเมลหรือที่เกี่ยวข้องกับแหล่งแพร่มัลแวร์ (Symantec, n.d.).

๓) แฮชไฟล์ (File Hashes) การตรวจจับไฟล์ที่เป็นมัลแวร์โดยใช้แฮช เช่น MD5 หรือ SHA-256 ที่เป็นที่รู้จักในฐานข้อมูลมัลแวร์

๔) พฤติกรรมของระบบที่ผิดปกติ เช่น การส่งข้อมูลจำนวนมากออกจากเครือข่ายในช่วงเวลาสั้น (Data Exfiltration) หรือการติดตั้งโปรแกรมโดยไม่ทราบที่มา (SANS Institute, 2019).

๕) ลายเซ็นหรือร่องรอยของมัลแวร์ เช่น รูปแบบการเขียนหรือคำสั่งในโค้ดที่ใช้โดยมัลแวร์บางชนิด

๓) การเปลี่ยนแปลงไฟล์หรือระบบที่ไม่คาดคิด เช่น การเปลี่ยนแปลงการตั้งค่า Registry หรือการสร้างไฟล์ที่ไม่รู้จักในระบบ

IoC เป็นองค์ประกอบสำคัญใน Threat Hunting และ Incident Response โดยช่วยให้นักวิเคราะห์ความปลอดภัยสามารถระบุและติดตามภัยคุกคามในระบบได้รวดเร็วขึ้น และป้องกันความเสียหายเพิ่มเติมโดยการกำจัดภัยคุกคาม รวมถึงเพิ่มความสามารถในการคาดการณ์และป้องกันการโจมตีในอนาคต

ในปัจจุบัน มีการใช้งาน IoC ในกระบวนการรักษาความมั่นคงปลอดภัยไซเบอร์ ไม่ว่าจะเป็นการตรวจจับภัยคุกคาม เช่น Intrusion Detection Systems (IDS) หรือ Endpoint Detection and Response (EDR) ใช้ IoC ในการระบุภัยคุกคามที่อาจเกิดขึ้น นอกจากนี้ยังใช้เพื่อการตอบสนองต่อเหตุการณ์ (Incident Response) IoC ช่วยในกระบวนการวิเคราะห์และกักกันการโจมตี เช่น การบล็อก IP หรือการลบไฟล์มัลแวร์ (Kaspersky, n.d.) และการแบ่งปันข้อมูลภัยคุกคาม (Threat Intelligence Sharing) IoC สามารถแบ่งปันระหว่างองค์กรหรือในเครือข่ายอุตสาหกรรมเพื่อป้องกันภัยคุกคามที่คล้ายกัน (Symantec, n.d.).

การตรวจจับภัยคุกคามถือเป็นสิ่งแรกและเป็นสิ่งที่มีความสำคัญต่อการรับมือภัยคุกคามทางไซเบอร์ โดยสามารถใช้ IoC ในการเป็นคุณลักษณะ (Features) ที่สำคัญในการตรวจจับ โดย IoC ที่นิยมใช้ในปัจจุบันจำนวน ๑๕ คุณลักษณะ (SentinelOne, n.d.) (Microsoft, n.d.) (MFEC, n.d.). ประกอบด้วย

๑) ปริมาณการรับส่งข้อมูลขาออกที่ผิดปกติ การเพิ่มขึ้นอย่างฉับพลันของข้อมูลที่ส่งออกจากเครือข่ายอาจบ่งชี้ถึงการขโมยข้อมูลหรือกิจกรรมที่ไม่พึงประสงค์

๒) การพยายามลงชื่อเข้าใช้ที่ล้มเหลวหลายครั้ง การพยายามเข้าสู่ระบบที่ล้มเหลวซ้ำ ๆ อาจเป็นสัญญาณของการพยายามเจาะระบบด้วยวิธี Brute Force

๓) การเปลี่ยนแปลงไฟล์หรือระบบที่ไม่คาดคิด การปรับเปลี่ยนไฟล์หรือการตั้งค่าระบบโดยไม่ได้รับอนุญาตอาจบ่งชี้ถึงการติดตั้งมัลแวร์หรือการเข้าถึงที่ไม่ได้รับอนุญาต

๔) การติดตั้งซอฟต์แวร์ที่ไม่รู้จักหรือไม่ได้รับอนุญาต การปรากฏของโปรแกรมที่ไม่ทราบที่มาอาจเป็นสัญญาณของการติดตั้งมัลแวร์

๕) การเชื่อมต่อกับที่อยู่ IP หรือโดเมนที่น่าสงสัย การสื่อสารกับเซิร์ฟเวอร์ที่เกี่ยวข้องกับกิจกรรมอันตรายอาจบ่งชี้ถึงการควบคุมจากภายนอก

๖) การใช้โปรโตคอลที่ไม่ปกติหรือพอร์ตที่ไม่คุ้นเคย การใช้พอร์ตหรือโปรโตคอลที่ไม่สอดคล้องกับการดำเนินงานปกติอาจเป็นสัญญาณของกิจกรรมที่น่าสงสัย

๗) การเปลี่ยนแปลงการกำหนดค่าระบบโดยไม่ได้รับอนุญาต การปรับแต่งการตั้งค่าระบบโดยไม่ได้รับอนุญาตอาจบ่งชี้ถึงการพยายามควบคุมระบบ

๘) การสร้างหรือแก้ไขบัญชีผู้ใช้โดยไม่ทราบสาเหตุ การมีบัญชีผู้ใช้ใหม่หรือการเปลี่ยนแปลงสิทธิ์โดยไม่ทราบที่มาอาจเป็นสัญญาณของการบุกรุก

๙) การทำงานของโปรเซสที่ไม่คุ้นเคยหรือผิดปกติ การปรากฏของโปรเซสที่ไม่รู้จักหรือการทำงานที่ผิดปกติอาจบ่งชี้ถึงการติดมัลแวร์

๑๐) การเข้าถึงข้อมูลหรือระบบในเวลาที่ไม่ปกติ การเข้าถึงระบบในเวลาที่ไม่สอดคล้องกับการทำงานปกติอาจเป็นสัญญาณของการบุกรุก

๑๑) การส่งข้อมูลจำนวนมากไปยังปลายทางที่ไม่รู้จัก การส่งข้อมูลปริมาณมากไปยังที่อยู่ที่ไม่รู้จักอาจบ่งชี้ถึงการขโมยข้อมูล

๑๒) การใช้เครื่องมือหรือสคริปต์ที่ไม่ได้รับอนุญาต การใช้เครื่องมือที่ไม่ได้รับอนุญาตอาจเป็นสัญญาณของการพยายามเจาะระบบ

๑๓) การเปลี่ยนแปลงสิทธิ์ของไฟล์หรือโฟลเดอร์โดยไม่ทราบสาเหตุ การปรับเปลี่ยนสิทธิ์การเข้าถึงโดยไม่ได้รับอนุญาตอาจบ่งชี้ถึงการพยายามเข้าถึงข้อมูลที่สำคัญ

๑๔) การรับส่งข้อมูลกับประเทศที่ไม่มีการติดต่อธุรกิจ การสื่อสารกับที่อยู่ IP ในประเทศที่องค์กรไม่มีการดำเนินงานอาจเป็นสัญญาณของการบุกรุก

๑๕) การตรวจพบแฮชไฟล์ที่ตรงกับมัลแวร์ที่รู้จัก การพบไฟล์ที่มีแฮชตรงกับมัลแวร์ที่รู้จักอาจบ่งชี้ถึงการติดมัลแวร์ดังกล่าว

๒.๕ โมเดล Pyramid of Pain

Pyramid of Pain เป็นโมเดลในด้านความมั่นคงปลอดภัยไซเบอร์ที่ออกแบบโดย David J. Bianco เพื่อแสดงระดับความเจ็บปวด (หรือความยาก) ที่ผู้โจมตีจะต้องเผชิญเมื่อผู้ป้องกัน (Defender) ระบุและแก้ไข Indicator of Compromise (IoC) ในระบบของตน โมเดลนี้ช่วยให้ผู้ป้องกันเข้าใจว่า IoC ที่แตกต่างกันส่งผลกระทบต่อผู้โจมตีอย่างไร และควรโฟกัสที่ระดับใดเพื่อทำให้ผู้โจมตีใช้ทรัพยากรและเวลามากขึ้น (Bianco, 2013) ภาพที่ ๒.๓ แสดงโมเดล Pyramid of Pain แบ่ง IoCs ออกเป็น ๖ ระดับ เรียงจากระดับความง่ายที่สุดไปยังยากที่สุด ดังนี้:

๑) Hash Values (ค่าแฮช) มีระดับความยากอยู่ที่ระดับต่ำสุด เช่น ค่า MD5, SHA-256 ที่ระบุไฟล์มัลแวร์ การเปลี่ยนค่าแฮชทำได้ง่ายโดยผู้โจมตี จึงมีผลกระทบน้อย

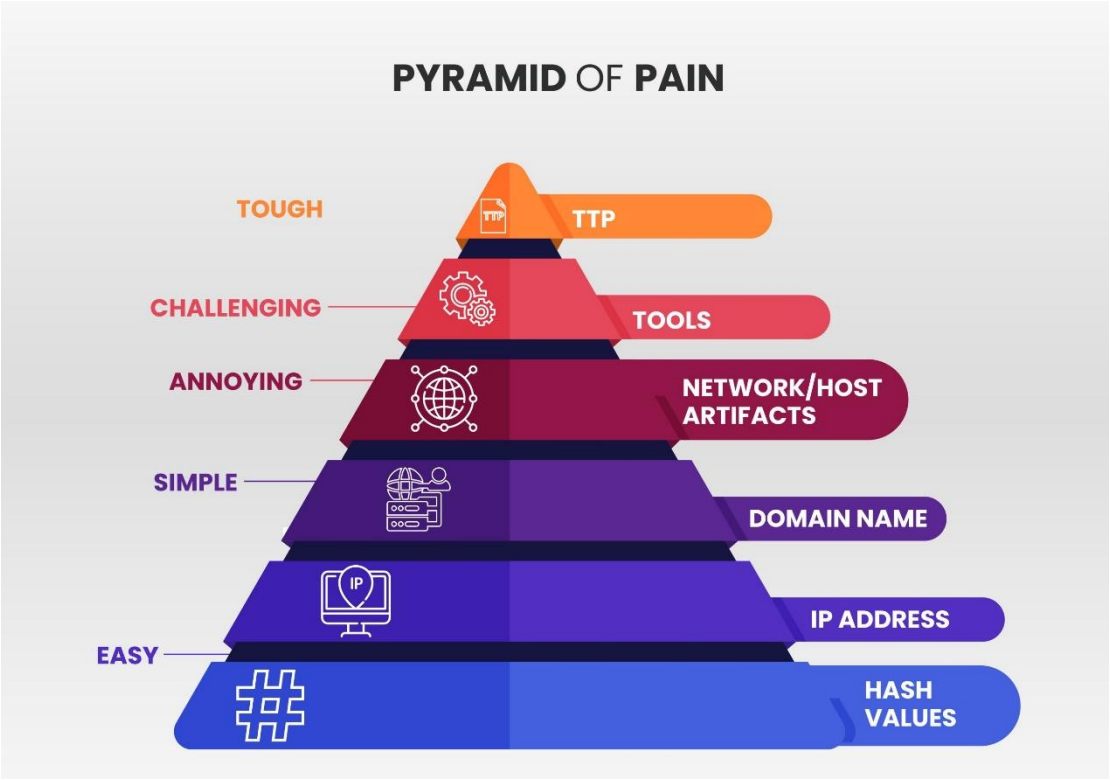
๒) IP Addresses (ที่อยู่ IP) การบล็อก IP ที่เกี่ยวข้องกับภัยคุกคาม เช่น Command and Control (C2) แม้จะง่ายต่อการเปลี่ยนแปลง แต่ช่วยลดความเสี่ยงได้ในระดับหนึ่ง

๓) Domain Names (ชื่อโดเมน) การบล็อกชื่อโดเมนที่น่าสงสัย เช่น ที่ใช้ในฟิชชิ่ง ผู้โจมตีต้องลงทะเบียนโดเมนใหม่หากโดเมนเก่าถูกบล็อก ซึ่งเริ่มเพิ่มค่าใช้จ่าย

๔) Network/Host Artifacts (ร่องรอยเครือข่ายหรือระบบ) การตรวจจับกิจกรรมที่ผิดปกติในระบบ เช่น รูปแบบทราฟฟิกที่ผิดปกติ ผู้โจมตีต้องปรับเปลี่ยนพฤติกรรมของมัลแวร์หรือการโจมตีเพื่อหลบเลี่ยง

๕) Tools (เครื่องมือที่ใช้โจมตี) การตรวจจับและบล็อกเครื่องมือโจมตี เช่น Metasploit หรือ Cobalt Strike ทำให้ผู้โจมตีต้องเปลี่ยนไปใช้เครื่องมือใหม่หรือพัฒนาเอง ซึ่งใช้ทรัพยากรมากขึ้น

๖) Tactics, Techniques, and Procedures (TTPs) การขัดขวางในระดับนี้ เช่น การเปลี่ยนกลยุทธ์การโจมตี ส่งผลกระทบมากที่สุด ผู้โจมตีต้องเปลี่ยนแปลงแผนการโจมตีและเสียเวลาอย่างมาก



ภาพที่ ๒.๓ โมเดล Pyramid of Pain[๘]

ผู้ดูแลระบบสามารถใช้ประโยชน์จากความเกี่ยวข้องกับความสัมพันธ์ของ IoCs แต่ละประเภทกับระดับความยากง่ายในโมเดล Pyramid of Pain เช่น IoCs ในระดับล่าง เช่น ค่าแฮชหรือ IP ส่งผลกระทบต่อผู้โจมตีได้น้อย แต่สามารถจัดการได้ง่ายและรวดเร็ว ในทางตรงกันข้าม IoCs ในระดับสูง เช่น TTPs ส่งผลกระทบต่อผู้โจมตีมากที่สุด แต่ต้องใช้ทรัพยากรในการวิเคราะห์และป้องกันมากขึ้น (SANS Institute, 2020) โดยมีตัวอย่างการใช้งาน อาทิ หากองค์กรตรวจจับและตอบสนอง

[๘] Bianco, D. (2013). *The Pyramid of Pain*. Retrieved from detect-respond.blogspot.com

ต่อ TTPs ได้ เช่น วิธีการเจาะระบบเฉพาะ จะทำให้ผู้โจมตีต้องปรับเปลี่ยนแผนการโจมตีใหม่ทั้งหมด ซึ่งเพิ่มค่าใช้จ่ายและลดความสามารถของผู้โจมตี (Bianco, 2013)

๒.๖ โมเดลภัยวิเคราะห์ความเสี่ยงจากภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์

ในโลกของความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) การทำความเข้าใจและจัดการกับ ภัยคุกคาม (Threats) และ ความเสี่ยง (Risks) เป็นสิ่งสำคัญอย่างยิ่ง การใช้ โมเดลภัยคุกคามและความเสี่ยง (Threat and Risk Models) ช่วยให้องค์กรสามารถระบุ วิเคราะห์ และจัดลำดับความสำคัญของภัยคุกคามที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ

การจัดการความเสี่ยงทางไซเบอร์ (Cyber Risk Management) เป็นกระบวนการที่สำคัญในการป้องกันและลดผลกระทบจากภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับองค์กร กระบวนการนี้ประกอบด้วยขั้นตอนหลัก ๆ ได้แก่ การระบุความเสี่ยง การวิเคราะห์ความเสี่ยง การควบคุมความเสี่ยง และการประเมินความเสี่ยง การทำความเข้าใจแต่ละขั้นตอนจะช่วยให้องค์กรสามารถจัดการกับความเสี่ยงได้อย่างมีประสิทธิภาพ โดยการจัดการความเสี่ยงทางไซเบอร์มีขั้นตอนในการดำเนินการดังนี้

๒.๖.๑ การระบุความเสี่ยง (Risk Identification)

เป็นขั้นตอนแรกในการระบุและบันทึกความเสี่ยงที่อาจส่งผลกระทบต่อสินทรัพย์ขององค์กร การระบุความเสี่ยงทางไซเบอร์รวมถึงการตรวจสอบช่องโหว่ในระบบ ความเสี่ยงจากบุคคลภายใน และภัยคุกคามจากภายนอก การใช้เครื่องมือและเทคนิคต่าง ๆ เช่น การตรวจสอบระบบและการวิเคราะห์ภัยคุกคาม ช่วยในการระบุความเสี่ยงที่อาจเกิดขึ้น (National Institute of Standards and Technology [NIST], 2020)

๒.๖.๒ การวิเคราะห์ความเสี่ยง (Risk Analysis)

หลังจากระบุความเสี่ยงแล้ว ขั้นตอนต่อไปคือการวิเคราะห์เพื่อประเมินความน่าจะเป็นและผลกระทบของแต่ละความเสี่ยง การวิเคราะห์นี้สามารถทำได้ทั้งในเชิงคุณภาพและเชิงปริมาณ โดยพิจารณาปัจจัยต่าง ๆ เช่น ความถี่ของการเกิดเหตุการณ์และความรุนแรงของผลกระทบ การวิเคราะห์ความเสี่ยงช่วยให้องค์กรเข้าใจถึงความสำคัญของแต่ละความเสี่ยงและจัดลำดับความสำคัญในการจัดการ (UpGuard, 2023)

๒.๖.๓ การควบคุมความเสี่ยง (Risk Control)

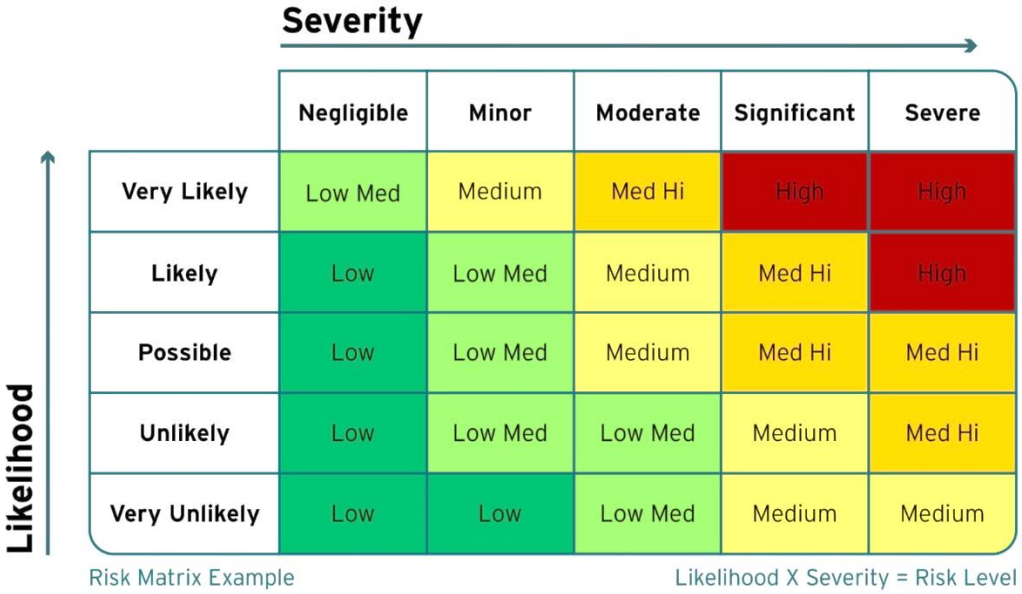
เป็นขั้นตอนที่องค์กรกำหนดมาตรการเพื่อลดหรือควบคุมความเสี่ยงที่ระบุและวิเคราะห์ไว้ มาตรการเหล่านี้อาจรวมถึงการติดตั้งระบบป้องกัน การฝึกอบรมพนักงาน หรือการพัฒนานโยบายความปลอดภัย การควบคุมความเสี่ยงมีวัตถุประสงค์เพื่อลดความน่าจะเป็นของการเกิดเหตุการณ์และลดผลกระทบที่อาจเกิดขึ้น (International Organization for Standardization [ISO], 2018)

๒.๖.๔ การประเมินความเสี่ยง (Risk Assessment)

เป็นกระบวนการที่รวมการระบุ การวิเคราะห์ และการประเมินความเสี่ยงเพื่อกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ การประเมินความเสี่ยงช่วยให้องค์กรตัดสินใจเกี่ยวกับ

มาตรการควบคุมที่เหมาะสมและจัดสรรทรัพยากรในการจัดการความเสี่ยงอย่างมีประสิทธิภาพ (Deloitte, 2021)

โดยในการประเมินความเสี่ยงนั้นถือเป็นขั้นตอนที่สำคัญในการจัดการความเสี่ยงภายในด้านความมั่นคงปลอดภัยไซเบอร์ โดยพิจารณาจากสองปัจจัยหลัก ได้แก่ โอกาสที่จะเกิดเหตุการณ์ (Likelihood) และ ความรุนแรงของผลกระทบ (Severity) การใช้ตารางความเสี่ยง (Risk Matrix) ดังแสดงในภาพที่ ๒.๔ ช่วยในการประเมินและจัดลำดับความสำคัญของความเสี่ยงแต่ละประเภทได้อย่างมีประสิทธิภาพ



ภาพที่ ๒.๔ ภาพตารางความเสี่ยง (Risk Matrix)[๙]

๒.๗ ภาษาไพธอน

ไพธอน (Python) เป็นภาษาโปรแกรมระดับสูงที่ออกแบบมาให้เรียนรู้และใช้งานได้ง่ายโดยมีลักษณะเด่นที่ความยืดหยุ่น การอ่านโค้ดที่เข้าใจง่าย สามารถทำงานในรูปแบบมัลติแพลตฟอร์ม Python ได้รับการพัฒนาโดย Guido van Rossum ในปี ๑๙๑๑ และปัจจุบันได้รับการยอมรับอย่างกว้างขวางในการใช้งานด้านความมั่นคงปลอดภัยไซเบอร์ (Python Software Foundation, 2023) Python มีจุดเด่นที่สำคัญ เช่น มีโครงสร้างภาษาที่เรียบง่าย มีไลบรารีและเฟรมเวิร์กจำนวนมากให้ใช้งาน มีชุมชนผู้ใช้งานขนาดใหญ่ รวมถึงรองรับการเขียนโปรแกรมทั้งแบบเชิงวัตถุ (Object-Oriented) และเชิงฟังก์ชัน (Functional Programming)

บทบาทของ Python ในงานด้าน Threat Intelligence พบว่ามีบทบาทสำคัญในหลายแง่มุม โดยเฉพาะในการจัดการกับ Threat Intelligence หรือการรวบรวม วิเคราะห์ และประเมินข้อมูลที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ดังนี้

[๙] https://www.riskpal.com/risk-assessment-matrices/

๒.๗.๑ การรวบรวมข้อมูล (Data Collection)

Python สามารถใช้เพื่อดึงข้อมูลจากแหล่งต่าง ๆ เช่น การดึงข้อมูล Threat Feeds หรือ API จากบริการ Threat Intelligence เช่น VirusTotal, Shodan, หรือ AlienVault รวมถึงการรวบรวมข้อมูลจากเว็บด้วย Web Scraping โดยใช้ไลบรารี เช่น BeautifulSoup, Scrapy (Alhazmi & Malaiya, 2014)

๒.๗.๒ การวิเคราะห์ข้อมูล (Data Analysis)

Python มีไลบรารีเช่น pandas, NumPy, และ matplotlib ที่ช่วยวิเคราะห์และแสดงผลข้อมูล เช่น การตรวจสอบความผิดปกติในกิจกรรมเครือข่าย รวมถึงการวิเคราะห์ข้อมูล IoC (Indicators of Compromise) เช่น ที่อยู่ IP, ชื่อโดเมน, หรือค่าแฮชของไฟล์ (Casey, 2015)

๒.๗.๓ การตรวจจับภัยคุกคาม (Threat Detection)

Python ช่วยพัฒนาสคริปต์สำหรับการค้นหาและตรวจจับรูปแบบการโจมตี และการวิเคราะห์พฤติกรรมมัลแวร์โดยใช้ไลบรารี เช่น pefile, pydeep (Schneider, 2017)

๒.๗.๔ การทำระบบอัตโนมัติ (Automation)

Python เป็นตัวเลือกที่เหมาะสมสำหรับการทำงานอัตโนมัติ เช่น การพัฒนาระบบเตือนภัย รวมถึงการสร้างสคริปต์สำหรับตอบสนองต่อเหตุการณ์ (SANS Institute, 2020)

๒.๗.๕ การทดสอบความปลอดภัย (Penetration Testing)

Python มีเฟรมเวิร์กและไลบรารี เช่น Scapy, Impacket, และ pwntools ที่ช่วยสร้างเครื่องมือสำหรับ การทดสอบเจาะระบบ รวมถึงการสร้างสคริปต์สำหรับการตรวจสอบช่องโหว่ (Alhazmi & Malaiya, 2014)

๒.๗.๖ การจัดการ Threat Intelligence

Python ช่วยจัดการและบูรณาการข้อมูล Threat Intelligence เช่น การรวมข้อมูลจากหลายแหล่ง การแสดงผลในรูปแบบรายงานหรือแดชบอร์ด (Casey, 2015)

๒.๘ Mern Stack

MERN Stack เป็นชุดเทคโนโลยีที่ใช้สำหรับพัฒนาเว็บแอปพลิเคชันแบบ Full-Stack ซึ่งมีความนิยมในกลุ่มนักพัฒนา เนื่องจากครอบคลุมทั้งฝั่ง Frontend และ Backend โดย MERN เป็นคำย่อที่มาจาก:

M – MongoDB: ฐานข้อมูลแบบ NoSQL ที่ใช้โครงสร้าง JSON-like สำหรับจัดการข้อมูล

E – Express.js: Framework ฝั่ง Backend ที่ทำงานบน Node.js ใช้สร้าง API และจัดการเซิร์ฟเวอร์

R – React.js: JavaScript Library ที่ใช้สร้าง User Interface ฝั่ง Frontend

N – Node.js: Runtime สำหรับ JavaScript ทำให้สามารถเขียนโค้ดฝั่งเซิร์ฟเวอร์ด้วย JavaScript

ดังนั้น MERN Stack จึงถือได้ว่าเป็นชุดเทคโนโลยีที่รวม MongoDB, Express.js, React.js, และ Node.js เข้าด้วยกัน ซึ่งเหมาะสำหรับการพัฒนาแอปพลิเคชันแบบ Full-Stack โดยเฉพาะอย่างยิ่งในงานด้าน Threat Intelligence (Sharma, 2020; Kumar, 2019). เพื่อพัฒนาเว็บแอปพลิเคชัน

แบบไดนามิกที่ต้องการความเร็ว และสามารถนำมาปรับใช้ในงานด้าน Threat Intelligence ได้หลายรูปแบบ โดยเน้นที่การพัฒนา Web-based Threat Intelligence Platforms ซึ่งสามารถรวบรวม วิเคราะห์ และแสดงผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ ดังนี้:

๒.๘.๑ การรวบรวมข้อมูล Threat Intelligence

- Backend (Node.js และ Express.js): ใช้พัฒนา API สำหรับเชื่อมต่อกับ Threat Intelligence Feeds เช่น VirusTotal หรือ AlienVault เพื่อทำการค้นหาข้อมูล IoC (Indicators of Compromise) เช่น IP, URL, หรือค่า Hash

- Database (MongoDB): เก็บข้อมูลภัยคุกคามในรูปแบบโครงสร้าง JSON เพื่อให้ง่ายต่อการจัดการและค้นหา

๒.๘.๒ การวิเคราะห์ข้อมูลภัยคุกคาม

- การพัฒนา Backend เพื่อรันการวิเคราะห์ข้อมูล เช่น การเปรียบเทียบ IP ที่น่าสงสัยกับฐานข้อมูล หรือการคำนวณความเสี่ยงจาก Threat Feeds

- การใช้ MongoDB ในการจัดการข้อมูลขนาดใหญ่ เช่น การบันทึกกิจกรรมเครือข่ายหรือการสร้างดัชนีของ IoC

๒.๘.๓ การแสดงผลข้อมูล Threat Intelligence

- Frontend (React.js): ใช้แสดงผลข้อมูลภัยคุกคามในรูปแบบ Dashboard ที่ผู้ใช้สามารถโต้ตอบได้ เช่น กราฟสถิติภัยคุกคาม รายงาน IoC และแผนที่ความสัมพันธ์ (Relationship Mapping)

- การพัฒนาเครื่องมือสำหรับการแจ้งเตือนแบบ Real-time เช่น การแจ้งเตือนเมื่อพบ IoC ที่เชื่อมโยงกับภัยคุกคามใหม่

๒.๘.๔ การทำระบบอัตโนมัติและการวิเคราะห์

Node.js: ใช้สำหรับตั้งเวลาการดึงข้อมูล Threat Feeds และอัปเดตฐานข้อมูลโดยอัตโนมัติ

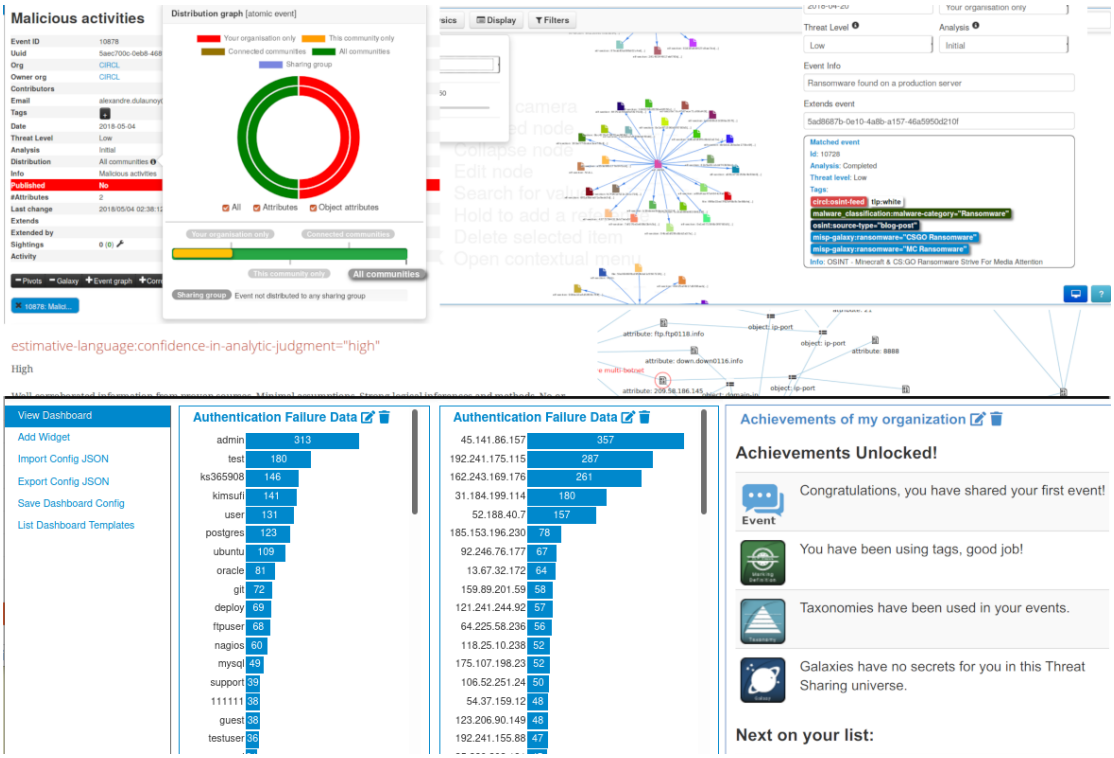
MongoDB และ Express.js: ใช้ประมวลผลและสร้างรายงานสรุปข้อมูลภัยคุกคาม

สำหรับตัวอย่างการประยุกต์ใช้ MERN Stack เช่น ใน Threat Intelligence Platform สามารถนำไปพัฒนาระบบสำหรับติดตามภัยคุกคามที่ดึงข้อมูลจาก Threat Feeds และแสดงผลในรูปแบบกราฟิก นอกจากนี้ยังสามารถนำไปใช้เป็น IoC Management Tool เพื่อเป็นเครื่องมือสำหรับบันทึกและติดตาม Indicators of Compromise โดยใช้ MongoDB เป็นฐานข้อมูล

๒.๙ Malware Information Sharing Platform

Malware Information Sharing Platform (MISP) เป็นโอเพนซอร์สแพลตฟอร์มที่ใช้สำหรับการจัดการและแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์ ในองค์กรหรือระหว่างกลุ่มองค์กร MISP ได้รับการพัฒนาเพื่อช่วยให้ทีมรักษาความปลอดภัยสามารถวิเคราะห์และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและมีประสิทธิภาพ (MISP Project, 2023) โดยมีฟีเจอร์หลักประกอบด้วย การรวบรวมข้อมูลภัยคุกคาม (Threat Data Collection) ซึ่งรองรับการบันทึก Indicators of Compromise (IoCs) เช่น IP, โดเมน, URL, ค่าแฮช และข้อมูลมัลแวร์, การแบ่งปันข้อมูล (Information Sharing)

ที่ช่วยสนับสนุนการแบ่งปันข้อมูลภัยคุกคามในกลุ่มที่เชื่อถือได้ เช่น CSIRTs, CERTs หรือพันธมิตรองค์กร, การวิเคราะห์ภัยคุกคาม (Threat Analysis) ซึ่งเป็นเครื่องมือช่วยวิเคราะห์ข้อมูลภัยคุกคาม เช่น การสร้างกราฟความสัมพันธ์ระหว่างเหตุการณ์หรือข้อมูล IoC, และการบูรณาการ (Integration) ที่สามารถเชื่อมต่อกับระบบอื่น ๆ เช่น SIEM (Security Information and Event Management) หรือ Threat Feeds



ภาพที่ ๒.๕ ภาพตัวอย่างการใช้งาน MISP[๑๐]

การใช้งาน MISP ในด้าน Threat Intelligence มีรูปแบบการดำเนินการประกอบด้วย

๒.๘.๑ การจัดการ IoC (Indicators of Compromise)

MISP ช่วยเก็บและจัดการ IoC ที่เกี่ยวข้องกับภัยคุกคาม เช่น: าแฮชของไฟล์ที่เป็นอันตราย ที่อยู่ IP ของเซิร์ฟเวอร์ Command and Control (C2) และโดเมนที่ใช้โจมตี (MISP Project, 2023)

๒.๘.๒ การแบ่งปันข้อมูลระหว่างองค์กร

MISP สนับสนุนการสร้างความร่วมมือระหว่างองค์กร เช่น การแบ่งปันข้อมูลภัยคุกคามระหว่างทีม CSIRT หรือ CERT รวมถึงการเผยแพร่ IoC ให้กับพันธมิตรเพื่อป้องกันภัยคุกคามใหม่ (Wagner et al., 2020)

---

[๑๐] https://www.misp-project.org/

๒.๘.๓ การสนับสนุนการวิเคราะห์

MISP ช่วยแสดงความสัมพันธ์ระหว่างเหตุการณ์ภัยคุกคาม เช่น การวิเคราะห์กราฟความเชื่อมโยงของ IoC รวมถึงการสร้าง Timeline เพื่อเข้าใจเหตุการณ์ย้อนหลัง (David, 2021).

๒.๘.๔ การบูรณาการกับระบบรักษาความปลอดภัย

MISP สามารถเชื่อมต่อกับเครื่องมืออื่น เช่น SIEM เช่น Splunk, Elastic Stack และ Threat Feeds เช่น VirusTotal, AlienVault OTX (Cohen & Stump, 2022)

MISP จึงถือเป็นแพลตฟอร์มที่สำคัญในงานด้าน Threat Intelligence ด้วยความสามารถในการจัดการ IoC การแบ่งปันข้อมูลดังแสดงในภาพที่ ๒.๕ และการวิเคราะห์ที่ครอบคลุม ทำให้องค์กรสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

๒.๑๐ OpenCTI

OpenCTI (Open Cyber Threat Intelligence) คือแพลตฟอร์มโอเพ่นซอร์สที่พัฒนาขึ้นเพื่อช่วยให้องค์กรสามารถจัดการ วิเคราะห์ และแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ (OpenCTI Documentation, 2023). แพลตฟอร์มนี้ถูกออกแบบมาเพื่อช่วยสร้าง Knowledge Graph ซึ่งเป็นโครงสร้างข้อมูลที่แสดงความสัมพันธ์ระหว่างตัวชี้วัดภัยคุกคาม (Indicators of Compromise: IoCs) และภัยคุกคาม (Threat Actors) รวมถึงเหตุการณ์ต่าง ๆ เพื่อให้ผู้ใช้สามารถเข้าใจภาพรวมของภัยคุกคามได้อย่างลึกซึ้ง (Bouchet et al., 2021). OpenCTI มีคุณสมบัติหลักดังนี้การจัดการข้อมูลภัยคุกคาม (OpenCTI Documentation, 2023).

๒.๑๐.๑ OpenCTI ช่วยให้ผู้ใช้สามารถเก็บและจัดการข้อมูลเกี่ยวกับภัยคุกคาม เช่น

- Indicators of Compromise (IoCs) เช่น IP Address, Domain, หรือค่า Hash
- Threat Actors เช่น กลุ่มแฮกเกอร์หรือผู้โจมตี
- Tactics, Techniques, and Procedures (TTPs) MITRE ATT&CK Framework

๒.๑๐.๒ การสร้างกราฟความรู้ (Knowledge Graph) แพลตฟอร์มนี้ช่วยแสดงความสัมพันธ์ระหว่างข้อมูลภัยคุกคาม เช่น

- การเชื่อมโยงระหว่าง Threat Actors และเหตุการณ์โจมตี
- การวิเคราะห์ลำดับการโจมตี (Bouchet et al., 2021).

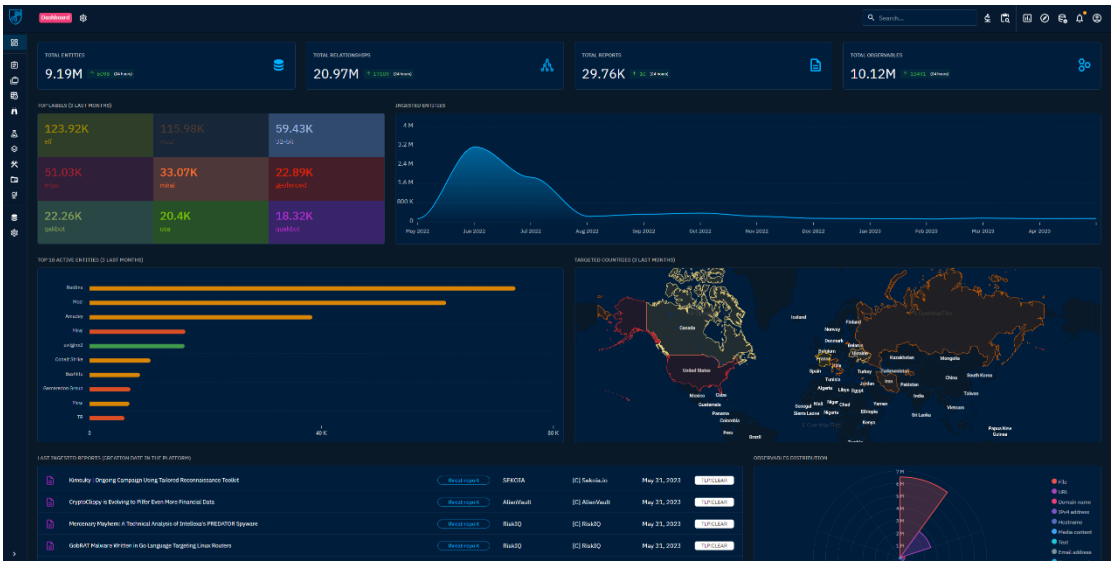
๒.๑๐.๓ การบูรณาการ (Integration) สามารถเชื่อมต่อกับเครื่องมือและระบบอื่น ๆ เช่น

- Threat Feeds: VirusTotal, AlienVault OTX
- SIEM (Security Information & Event Management) เช่น Splunk หรือ ELK Stack (OpenCTI Documentation, 2023).

๒.๑๐.๔ การแสดงผลข้อมูล OpenCTI มีแดชบอร์ดที่แสดงข้อมูลภัยคุกคามในรูปแบบภาพ เช่น กราฟความสัมพันธ์, Timeline และรายงานสรุป (OpenCTI Documentation, 2023).

สำหรับการนำ OpenCTI ไปใช้งานในปัจจุบัน มีการใช้งานอย่างแพร่หลายเพื่อสร้างระบบในการจัดการภัยคุกคามด้านไซเบอร์ภายในองค์กร เช่น การวิเคราะห์ภัยคุกคามในองค์กร โดยใช้ OpenCTI เพื่อจัดเก็บและวิเคราะห์ข้อมูล IoCs จากระบบเครือข่าย เช่น การตรวจจับ IP Address ที่น่าสงสัย และเชื่อมโยงกับฐานข้อมูลภัยคุกคาม (Bouchet et al., 2021) จากนั้นจึงทำการแบ่งปัน

ข้อมูลระหว่างองค์กร โดยแพลตฟอร์มนี้ช่วยให้ทีมรักษาความปลอดภัยแบ่งปันข้อมูลภัยคุกคามกับพันธมิตรหรือกลุ่ม CERT (Computer Emergency Response Team) ได้อย่างปลอดภัย (OpenCTI Documentation, 2023) มากไปกว่านั้น ยังสามารถใช้สำหรับการติดตามภัยคุกคามแบบเรียลไทม์ OpenCTI สามารถตั้งระบบแจ้งเตือนภัยคุกคามที่มีความสัมพันธ์กับข้อมูลในระบบขององค์กร (Bouchet et al., 2021).



ภาพที่ ๒.๖ ตัวอย่าง Interface ของ OpenCTI[๑๑]

ภาพที่ ๒.๖ แสดงตัวอย่าง Interface ของ OpenCTI จะเห็นว่า Knowledge Graph ที่สร้างโดย OpenCTI โดยมีการเชื่อมโยงข้อมูลภัยคุกคาม เช่น Threat Actors, IoCs และเหตุการณ์โจมตี ซึ่งช่วยให้นักวิเคราะห์สามารถเข้าใจความสัมพันธ์ระหว่างข้อมูลได้อย่างรวดเร็วและแม่นยำ (OpenCTI Documentation, 2023)

OpenCTI เป็นแพลตฟอร์มที่ทรงพลังสำหรับการจัดการและวิเคราะห์ข้อมูลภัยคุกคามที่ทันสมัย สามารถช่วยให้องค์กรเพิ่มประสิทธิภาพในการป้องกันและตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

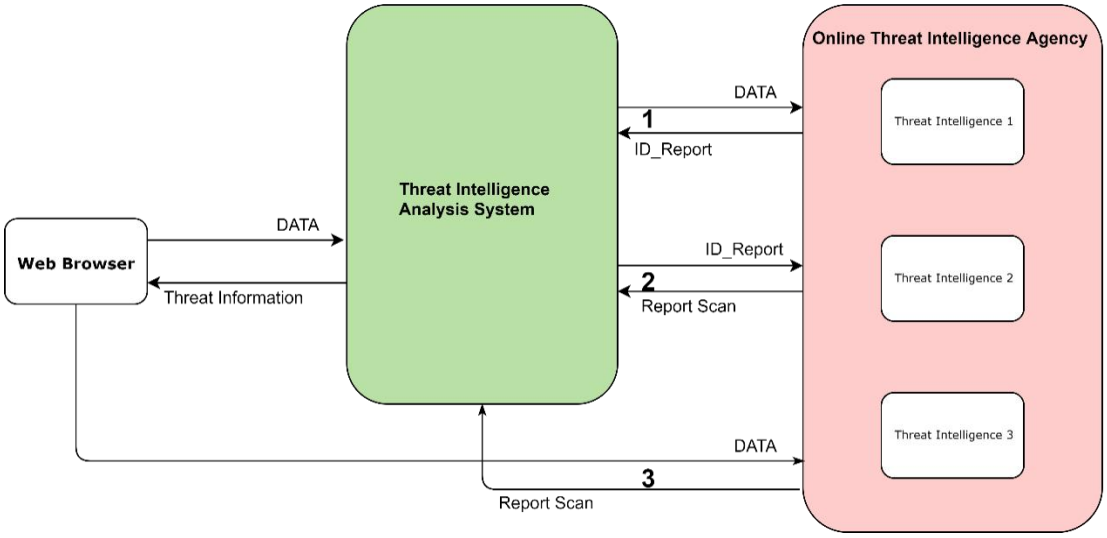
[๑๑] https://docs.opencti.io/5.7.X/usage/getting-started/

บทที่ ๓
วิธีดำเนินการวิจัย

๓.๑ แนวคิดการออกแบบระบบ

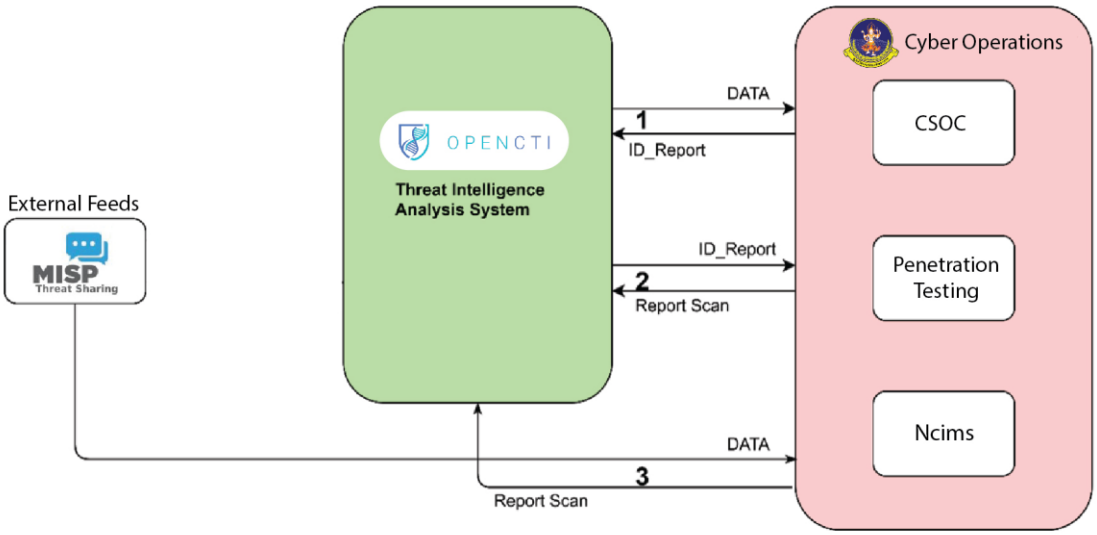
ในงานวิจัยนี้มีแนวคิดการออกแบบระบบงานที่มีพื้นฐานมาจากปัญหาที่เกิดขึ้นในการทำงานของหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ ที่ต้องใช้เวลาค่อนข้างนานในการค้นหาความสัมพันธ์ของภัยคุกคามที่เกิดขึ้นในระบบเพื่อเปรียบเทียบกับข้อมูล IOCs ที่มีการแชร์ข้อมูลบนระบบอินเทอร์เน็ตที่มีอย่างแพร่หลายจำนวนมาก โดยการนำข้อมูลเหล่านั้นไปสแกนหาความเสี่ยงจากแหล่งข้อมูลของผู้ให้บริการวิเคราะห์ภัยคุกคามออนไลน์

ถึงอย่างไรก็ตาม เนื่องจากข้อจำกัดที่ต้องหาข้อมูลจากหลายแหล่งมาช่วยในการตัดสินใจเกี่ยวกับภัยคุกคามที่เกิดขึ้น ทำให้ผู้ใช้งานหรือนักวิเคราะห์ภัยคุกคามที่ทำงานในศูนย์เฝ้าระวังความปลอดภัยคอมพิวเตอร์ (Computer Security Operations Center: CSOC) จะต้องเสียเวลาไปกับงานประจำในรูปแบบเดิมในทุกครั้งของการทำงาน เนื่องจากข้อมูล IOCs มีการแชร์ข้อมูลบนระบบอินเทอร์เน็ตมีอยู่เป็นจำนวนมากจากองค์กรที่เกี่ยวข้องกับข่าวกรองภัยคุกคามในระบบออนไลน์ (Online Threat Intelligence Agency) ดังแสดงในภาพที่ ๓.๑ จึงจำเป็นอย่างยิ่งที่ต้องมีการกรองข้อมูล เพื่อให้ได้เฉพาะข้อมูลที่มีความจำเป็นและมีประโยชน์ในการนำข้อมูลเหล่านั้นมาเพื่อใช้ในการตรวจสอบและพิสูจน์หลักฐานการบุกรุกเครือข่าย



ภาพที่ ๓.๑ แนวคิดของระบบงานเดิม

ระบบวิเคราะห์ข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์เป็นระบบที่ช่วยรวบรวมข้อมูล IOCs จากแหล่งข้อมูลเปิดและส่งไปสแกนยังผู้ให้บริการ Online Analysis เพื่อทำการวิเคราะห์ถึงภัยคุกคามของข้อมูล IOCs นั้น แล้วเก็บผลการวิเคราะห์มายังระบบ เพื่อเปรียบเทียบค่าความเสี่ยงและคำนวณค่าความเสี่ยงโดยรวมของภัยคุกคามนั้นซึ่งสามารถ ออกแบบระบบงานใหม่ขึ้นมาได้ดังภาพที่ ๓.๒ ที่มีการประยุกต์ใช้งาน OpenCTI เพื่อเป็นสื่อการในการประมวลผลเพื่อรับมือกับภัยคุกคามที่เกิดขึ้น



ภาพที่ ๓.๒ แนวคิดของระบบงานใหม่

๓.๒ ระบบในภาพรวม

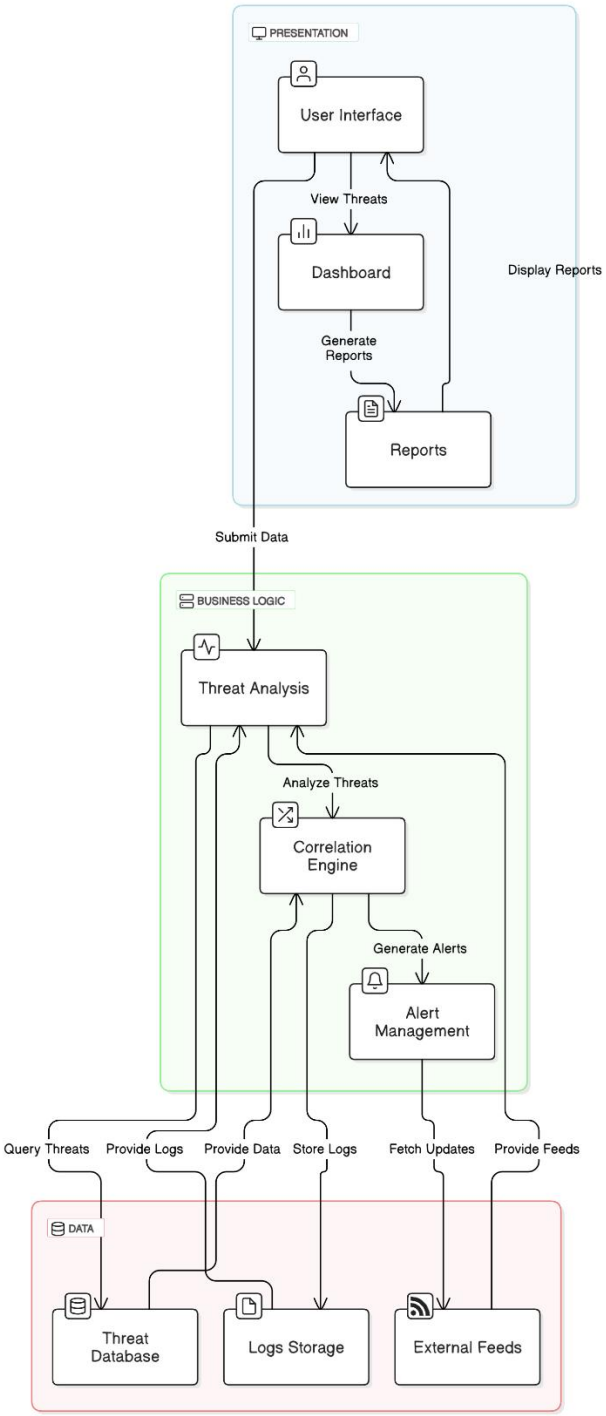
งานวิจัยนี้ใช้การออกแบบระบบในภาพรวมสถาปัตยกรรมแบบสามชั้น (3-Tier Architecture) เป็นรูปแบบการออกแบบระบบที่แบ่งการทำงานออกเป็นสามชั้นหลัก ได้แก่ ชั้นการนำเสนอ (Presentation Layer), ชั้นตรรกะธุรกิจ (Business Logic Layer) และชั้นข้อมูล (Data Layer) การแบ่งชั้นเช่นนี้ช่วยให้ระบบมีความยืดหยุ่น ง่ายต่อการบำรุงรักษา และสามารถปรับปรุงหรือขยายระบบได้โดยไม่ส่งผลกระทบต่อส่วนอื่น ๆ สำหรับระบบข่าวกรองภัยคุกคามไซเบอร์นี้ประยุกต์ใช้สถาปัตยกรรมแบบสามชั้นดังแสดงในภาพที่ ๓.๓ โดยแต่ละชั้นมีบทบาทดังนี้

๓.๒.๑ ชั้นการนำเสนอ (Presentation Layer) เป็นส่วนที่ผู้ใช้โต้ตอบกับระบบ ผ่านอินเทอร์เฟซผู้ใช้ เช่น แดชบอร์ด รายงาน และการแจ้งเตือน เพื่อแสดงข้อมูลและผลการวิเคราะห์ภัยคุกคาม

๓.๒.๒ ชั้นตรรกะธุรกิจ (Business Logic Layer): ทำหน้าที่ประมวลผลข้อมูลข่าวกรองภัยคุกคาม วิเคราะห์ความเสี่ยง และกำหนดมาตรการตอบสนองต่อภัยคุกคามที่ตรวจพบ

๒.๒.๓ ชั้นข้อมูล (Data Layer): จัดเก็บและจัดการข้อมูลที่เกี่ยวข้องกับภัยคุกคาม เช่น Indicators of Compromise (IoCs) ข้อมูลจากแหล่งข่าวกรอง และบันทึกเหตุการณ์ความปลอดภัย

การใช้สถาปัตยกรรมแบบสามชั้นในระบบข่าวกรองภัยคุกคามไซเบอร์ช่วยให้การจัดการและประมวลผลข้อมูลเป็นไปอย่างมีประสิทธิภาพ และสามารถปรับปรุงหรือขยายระบบได้ตามความต้องการขององค์กร



ภาพที่ ๓.๓ โครงสร้างแสดงการทำงานโดยรวมของระบบ

๓.๓ โครงสร้างการทำงานของระบบ

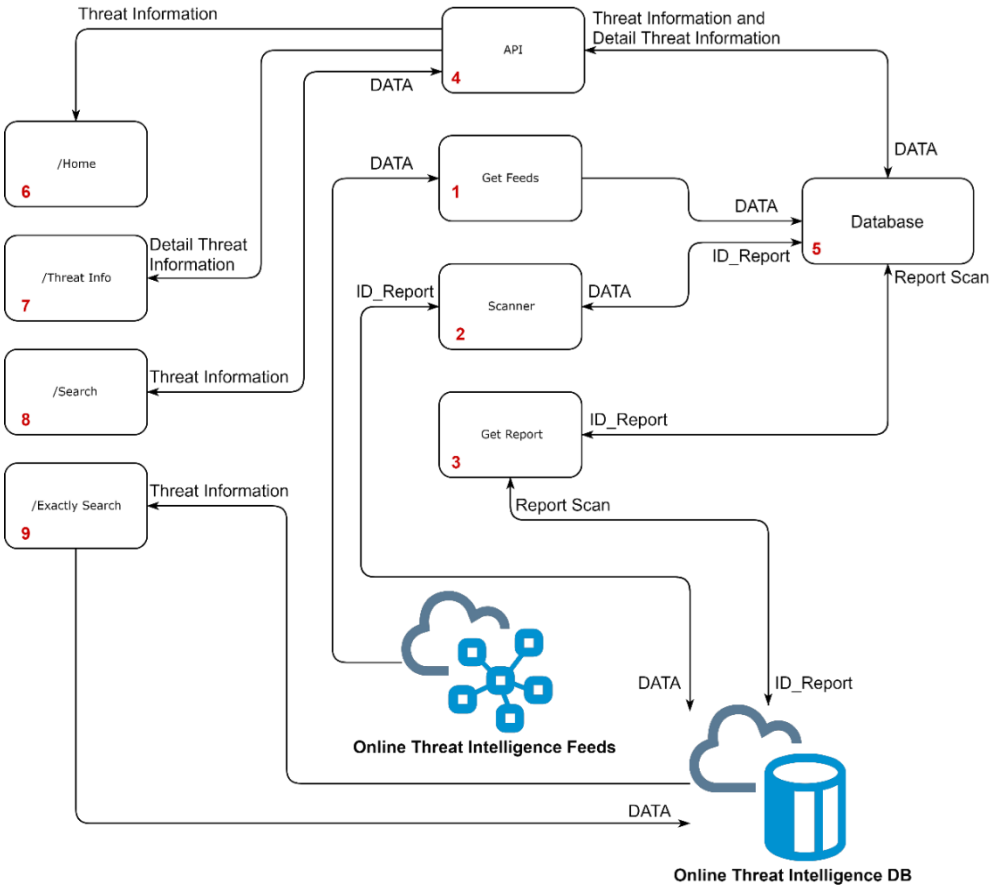
การทำงานโดยรวมของระบบมีฟังก์ชันการทำงาน โดยที่ผู้ใช้งานป้อนข้อมูลที่ต้องการค้นหาเข้ามาในระบบวิเคราะห์ภัยคุกคามทางไซเบอร์ หลังจากนั้นตัวระบบจะนำข้อมูลดังกล่าวไปค้นหาข้อมูลตามที่ผู้ใช้ต้องการจากระบบของผู้ให้บริการวิเคราะห์ภัยคุกคามออนไลน์ OPENCTI ซึ่งแบ่งออกเป็น ๓ ฟังก์ชันและทำงานต่อเนื่องกันตามลำดับโดยมีรายละเอียดดังนี้

๓.๓.๑ ระบบวิเคราะห์ภัยคุกคามทางไซเบอร์

ระบบทำการรับข้อมูลและส่งข้อมูลไปค้นหาจากระบบของผู้ให้บริการวิเคราะห์ภัยคุกคามออนไลน์แล้วส่งค่ากลับมาแค่รหัสของรายงาน การสแกนเท่านั้น

๓.๓.๒ ระบบวิเคราะห์ภัยคุกคามทางไซเบอร์

ระบบส่งรหัสของรายงานการสแกนไปดึงผลรายงาน การสแกนมาบันทึกลงในระบบและส่งผลกลับไปทาง External Feed MISP



ภาพที่ ๓.๔ การทำงานแอปพลิเคชันของระบบ

๓.๓.๓ ถ้า MISP ถูกใช้งานการค้นหาข้อมูลโดยระบุคีย์เวิร์ดค้นหาที่เฉพาะเจาะจงคำสั่งในการค้นหาจะถูกส่งไปยังระบบของผู้ให้บริการวิเคราะห์ภัยคุกคามออนไลน์ทันทีและส่งผลการค้นหา

กลับมาบันทึกลงในระบบวิเคราะห์ภัยคุกคามทางไซเบอร์ พร้อมกับส่งผลกลับไปทางเว็บเบราว์เซอร์ โดยส่งค่าของข้อมูลในแต่ละฟังก์ชันดังแสดงในภาพที่ ๓.๔ และมีรายละเอียดแต่ละขั้นตอนดังนี้

๑) Get Feeds คือ ฟังก์ชันที่ไปดึงข้อมูลภัยคุกคาม เช่น หมายเลขไอพี โดเมน ยูอาร์แอล และค่าแฮช จากระบบของผู้ให้บริการวิเคราะห์ภัยคุกคามออนไลน์มาเก็บลงในฐานข้อมูล

๒) Scanner คือ ฟังก์ชันที่ใช้ในการดึงข้อมูลที่อยู่ในฐานข้อมูลไปสแกนที่ระบบของผู้ให้บริการวิเคราะห์ภัยคุกคามออนไลน์แล้วตอบค่ากลับมาเป็น ID_Report เก็บลงในฐานข้อมูลซึ่ง ID_Report เป็นรหัสที่เอาไว้ใช้ดึงผลรายงานการสแกนจาก ระบบของผู้ให้บริการวิเคราะห์ภัยคุกคามออนไลน์

๓) Get Report คือ ฟังก์ชันที่ดึงค่า ID_Report เพื่อไปดึงรายงานการสแกนจากระบบของผู้ให้บริการวิเคราะห์ภัยคุกคามออนไลน์มาเก็บลงในฐานข้อมูล

๔) API หรือ เอพีไอ เป็นฟังก์ชันที่เป็นตัวกลางในการเชื่อมต่อกับฐานข้อมูล เพื่อดึงข้อมูลไปแสดงผลยังหน้า /Home, /Threat Info และรับข้อมูลจากหน้า /Search เพื่อไปค้นหาข้อมูลแล้วนำกลับไปแสดงผลยังหน้า /Search

๕) Database คือ ระบบฐานข้อมูลที่จัดเก็บข้อมูลของระบบทั้งหมด

๖) Home คือ หน้าเว็บที่แสดงผลให้กับผู้ใช้งาน

๗) Threat Info คือหน้าเว็บที่ทำการแสดงรายละเอียดของภัยคุกคาม

๘) Search คือ หน้าเว็บที่รับข้อมูลการค้นหาจากผู้ใช้งานและแสดงผล

๙) Exactly Search คือ ระบบ MISP ที่รับข้อมูลการค้นหาแบบเฉพาะเจาะจง โดยฟังก์ชันนี้จะไปค้นหาข้อมูลจากระบบของผู้ให้บริการวิเคราะห์ภัยคุกคามออนไลน์ มาแสดงผลให้ผู้ใช้งานพร้อมกับบันทึกผลที่ได้ลงในระบบฐานข้อมูลด้วย หากข้อมูลที่ได้มานั้นมีอยู่ในฐานข้อมูลแล้วจะทำการอัปเดตข้อมูลลงฐานข้อมูลเท่านั้น แต่ถ้าข้อมูลที่ได้มายังไม่มีในระบบก็ทำการบันทึกเข้าไปในฐานข้อมูลทันที ซึ่งฟังก์ชันการทำงานนี้จะเป็นการบันทึกและอัปเดต ข้อมูลลงในฐานข้อมูลทุกครั้งที่มีการใช้งาน

๓.๔ การออกแบบการไหลของกระบวนการ

การออกแบบการไหลของกระบวนการ (Process Flow) มีรายละเอียดและขั้นตอนการดำเนินการดังนี้

๓.๔.๑ โครงสร้างของระบบที่ได้ออกแบบไว้ตามหลัก 3-tiers คือแยกระบบการทำงานของแต่ละส่วนออกจากกัน สามารถแบ่งการทำงานของแต่ละส่วนได้ดังนี้

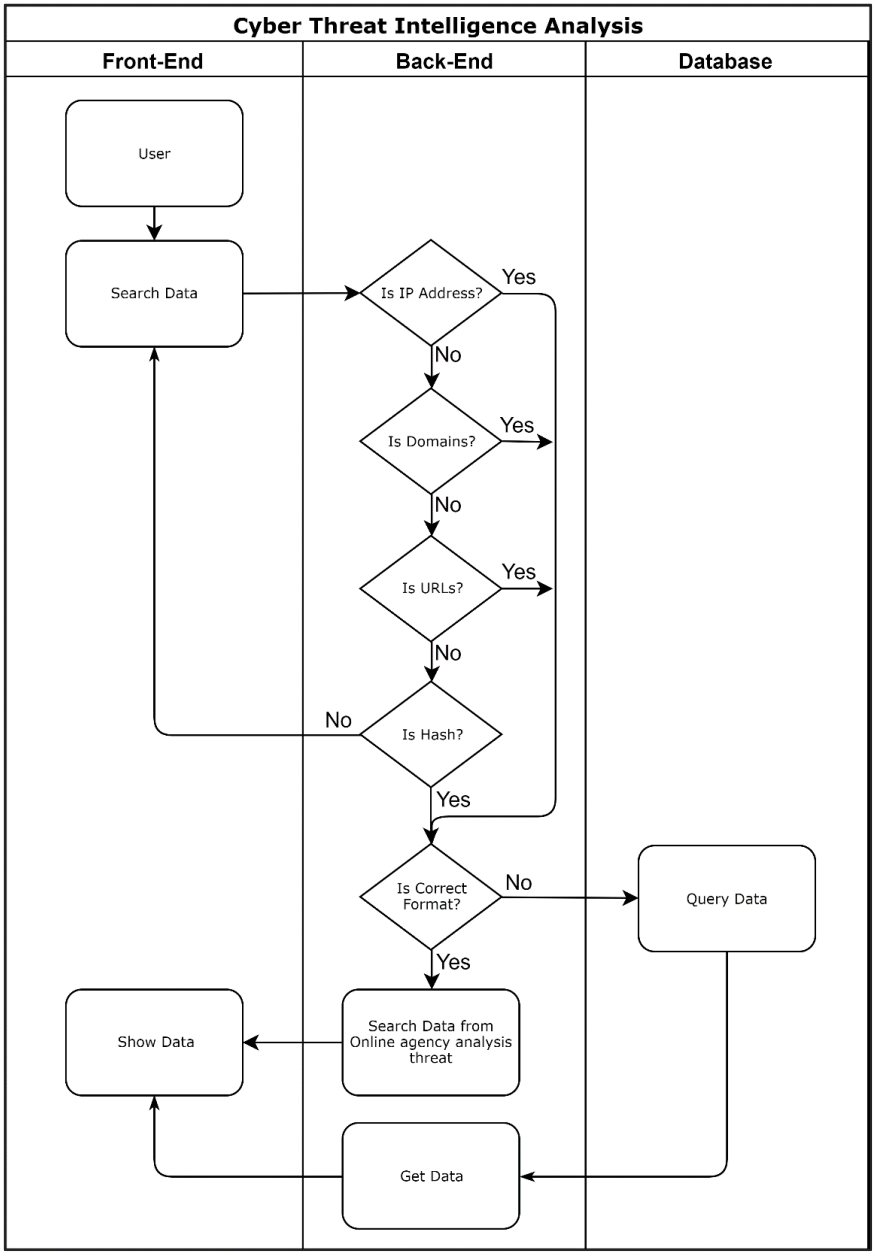
๑) ผู้ใช้งาน (User) คือผู้ที่ต้องการเข้ามาใช้งานระบบเพื่อค้นหาข้อมูลภัย คุกคามในระบบวิเคราะห์ภัยคุกคามทางไซเบอร์

๒) Front-End Server หรือเว็บเซิร์ฟเวอร์ที่เชื่อมต่อกับเอพีไอที่อยู่ในส่วนของ Back-End Server เพื่อนำข้อมูลมาแสดงบนเว็บเบราว์เซอร์และคอยให้บริการกับผู้ใช้งาน ระบบวิเคราะห์ภัยคุกคามทางไซเบอร์

๓) Back-End Server คือระบบในการบริหารจัดการขั้นตอนการทำงานของแต่ละกระบวนการตั้งแต่ขั้นตอนการดึงข้อมูลภัยคุกคามจากแหล่งข้อมูลเปิดแล้วเก็บลงใน ระบบฐานข้อมูล

การนำข้อมูลภัยคุกคามส่งไปสแกนยังผู้ให้บริการวิเคราะห์ภัยคุกคาม ออนไลน์เพื่อทำการวิเคราะห์ถึงภัยคุกคามของข้อมูลนั้น แล้วเก็บผลการวิเคราะห์มายังระบบ เพื่อเปรียบเทียบค่าความเสี่ยง คำนวณค่าความเสี่ยงโดยรวมของภัยคุกคามและเป็นตัวกลาง ในการรับค่าคำสั่งจาก Front-End Server ในการเชื่อมต่อกับระบบฐานข้อมูล

๔) Database Server คือเครื่องเซิร์ฟเวอร์ที่ให้บริการเก็บข้อมูลภัยคุกคามวัน เวลาที่มีการอัปเดตข้อมูล, แหล่งข้อมูลต้นทางที่ใช้ดึงข้อมูลภัยคุกคาม



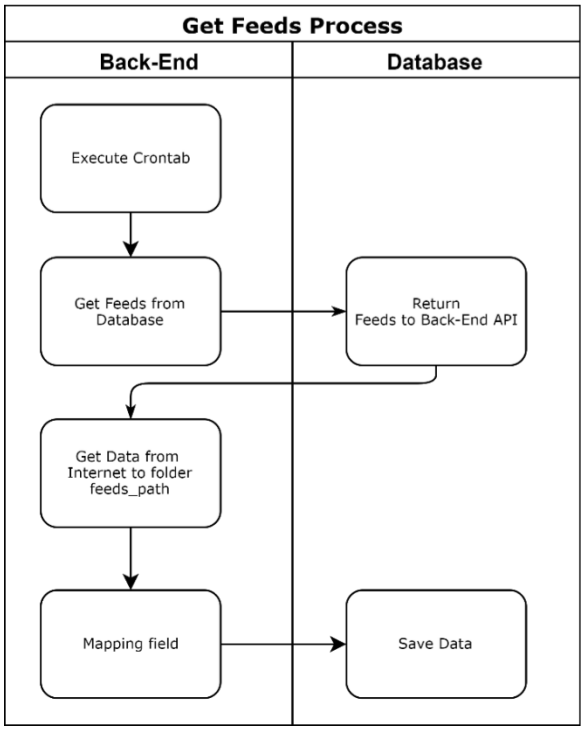
ภาพที่ ๓.๕ การไหลของกระบวนการเพื่อแสดงการทำงานโดยรวมของระบบ

๓.๔.๒ การออกแบบการไหลของกระบวนการเพื่อแสดงการทำงานโดยรวมของระบบสามารถจำแนกฟังก์ชันออกได้ดังนี้

๑) Front-End รับข้อมูลที่ผู้ใช้ร้องขอโดยสามารถค้นหาข้อมูล IOCs จากผู้ให้บริการระบบ Cyber Threat Intelligence Analysis

๒) Back-End ทำหน้าที่เป็นเอพีไอติดต่อกับฐานข้อมูล และอินเทอร์เน็ตในการค้นหาข้อมูลที่ผู้ใช้ร้องขอ เมื่อได้รับข้อมูลมาแล้ว เอพีไอจะมีเงื่อนไขในการตรวจสอบข้อมูลดังนี้

- ตรวจสอบประเภทของข้อมูลหมายเลขไอพีโดเมนยูอาร์แอลค่าแฮช
- ตรวจสอบความถูกต้องของรูปแบบประเภทข้อมูลถ้าไม่ถูกต้องระบบจะทำการค้นหาข้อมูลที่มีอยู่ในฐานข้อมูลขึ้นมาแสดงให้เลือก ๕๐ รายการจากข้อมูลทั้งหมดที่มีในระบบเพื่อให้ผู้ใช้เลือกรายการที่ถูกต้อง
- ถ้าเอพีไอตรวจพบว่าข้อมูลที่ผู้ใช้ป้อนเข้านั้น ถูกต้องตามรูปแบบของประเภทข้อมูลนั้น เอพีไอจะส่งข้อมูลที่ผู้ใช้ป้อนเข้ามาไปสแกนผลจากผู้ให้บริการ วิเคราะห์ภัยคุกคามออนไลน์ที่มีการเชื่อมต่อไว้ และดึงผลการสแกนดังกล่าวมา ถ้าข้อมูลนั่นมีอยู่แล้วจะไปอัปเดตลงในฐานข้อมูล แต่ถ้าไม่เคยมีข้อมูลมาก่อนจะทำการเพิ่มข้อมูลลงในฐานข้อมูลก่อน แล้วจึงส่งผลการสแกนดังกล่าวต่อให้ระบบ Front-End เพื่อแสดงรายละเอียดข้อมูลให้ผู้ใช้งาน โดยรายละเอียดทั้งหมดสามารถเขียนเป็นการ ไหลของกระบวนการได้ดังรูปภาพที่ ๓.๕ การไหลของกระบวนการเพื่อแสดงการทำงานโดยรวมของระบบ



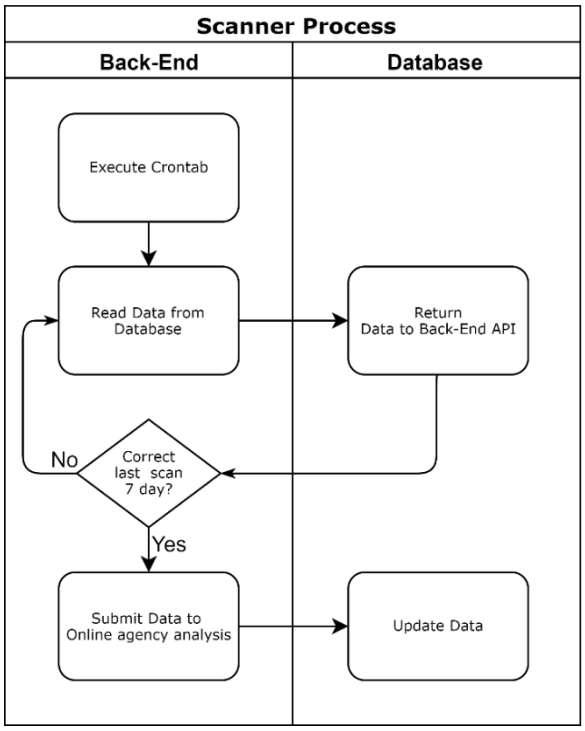
ภาพที่ ๓.๖ แสดงขั้นตอนการดึงข้อมูล Feeds

๓.๔.๓ การออกแบบการไหลของกระบวนการในขั้นตอนการดึงข้อมูลดึงข้อมูลจากออนไลน์

ภาพที่ ๓.๖ ที่แสดงตอนการดึงข้อมูล IOCs จากแหล่งข้อมูลออนไลน์โดยกระบวนการในขั้นตอนนี้จะถูกตั้ง Crontab เพื่อระบุเวลาที่จะไปดึงข้อมูลวันละครั้งในเวลา ๐๓.๐๐ น. เนื่องจากมี ข้อจำกัดในการดึงข้อมูลจากแหล่งข้อมูลเปิดออนไลน์มีจำกัด และเพื่อเป็นการบริหารจัดการระบบในการใช้งานทรัพยากรระบบให้เพียงพอกับที่ได้จัดสรรไว้ ซึ่งจะดึงข้อมูลจากแหล่งข้อมูลต้นทางที่มีการระบุไว้ในฐานข้อมูลเท่านั้น เมื่อดึงข้อมูลมาแล้วจะพักไว้ที่ feeds_path ก่อนแล้วจึงนำข้อมูลไปทำ การจัดรูปแบบก่อนที่จะบันทึกลงในฐานข้อมูล

๓.๔.๔ การออกแบบการไหลของกระบวนการเพื่อแสดงขั้นตอนการสแกน

ภาพที่ ๓.๗ เป็นขั้นตอนการดึงข้อมูลที่ถูกบันทึกลงในฐานข้อมูลโดยกระบวนการก่อนหน้า เพื่อนำข้อมูลไปสแกนยังผู้ให้บริการวิเคราะห์ภัยคุกคามออนไลน์ที่เราเลือกใช้บริการไว้ ซึ่งในกระบวนการทำงานของขั้นตอนนี้จะตั้งค่าเป็น Crontab ไว้เพื่อระบุเวลาในการทำงาน และมีข้อจำกัด ในเรื่องของจำนวนรายการที่นำไปสแกนจากทางผู้ให้บริการ ดังนั้นจึงต้องมีการตั้งค่าให้เลือกรายการข้อมูลที่ไม่ได้อัปเดตมาแล้ว ๗ วันขึ้นไปสแกนใหม่ในทุกวัน ในขั้นตอนนี้จะยังไม่ได้ผลการสแกนในทันที โดยจะเก็บบันทึกเพียงแค่รหัสของข้อมูลที่ได้จากการสแกนลงในฐานข้อมูลเท่านั้น

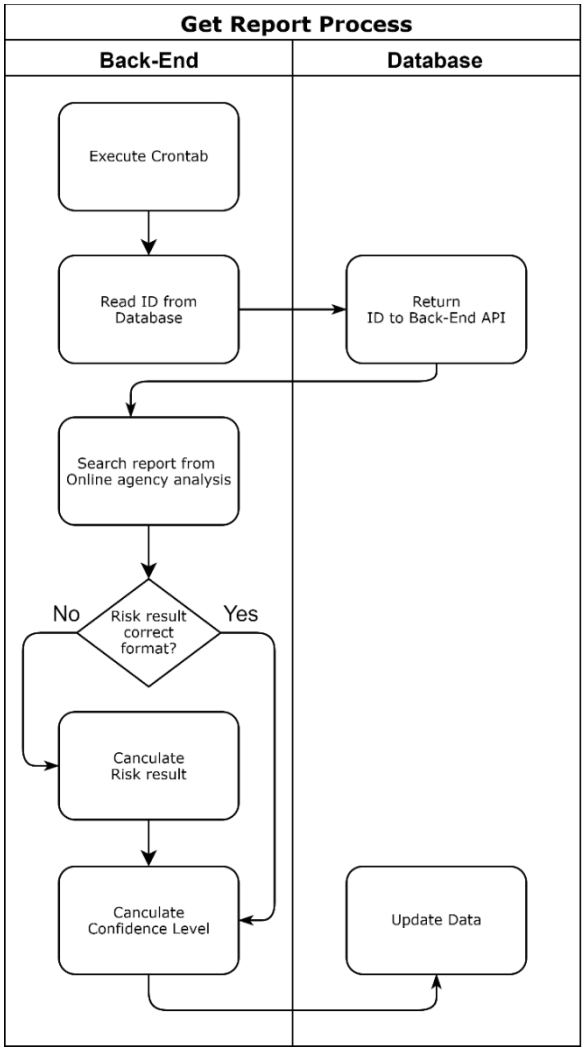


ภาพที่ ๓.๗ แสดงขั้นตอนการ Scan Process

๓.๔.๕ การออกแบบการไหลของกระบวนการเพื่อแสดงขั้นตอนการดึงรายงาน

ภาพที่ ๓.๘ แสดงขั้นตอนการดึงรายงานที่ได้จากการนำข้อมูลส่งไปสแกนยังผู้ให้บริการวิเคราะห์ภัยคุกคามออนไลน์ OPENCTI โดยกระบวนการก่อนหน้า และในกระบวนการทำงานของขั้นตอนนี้จะตั้งค่าเป็น Crontab ไว้เพื่อระบุเวลาในการทำงานไว้เช่นกัน ซึ่งจะเริ่มจากการ

ดึงรหัสของข้อมูลที่ได้จากการสแกนจากฐานข้อมูลมาก่อน แล้วนำไปค้นหาผลการสแกนจากผู้ให้บริการวิเคราะห์ภัยคุกคามออนไลน์ OPENCTI เมื่อได้ผลมาแล้วจะตรวจสอบก่อนว่าค่าของผลรวมความเสี่ยงที่ได้มาจากทั้ง ๓ แหล่งที่มานั้นอยู่ในรูปแบบเดียวกันหรือไม่ ถ้าไม่อยู่ในรูปแบบเดียวกันจะมีการคำนวณค่าใหม่เพื่อให้อยู่ในรูปแบบเดียวกันก่อน แล้วเอาค่าของผลรวมความเสี่ยงของแต่ละที่มาคำนวณหาระดับความเชื่อมั่น (Confidence Level) เพื่อเก็บข้อมูลไว้ ซึ่งระดับความเชื่อมั่นนี้จะเป็นค่าที่สามารถแก้ไขได้ภายหลัง เพื่อให้เหมาะสมกับการนำไปใช้งาน



ภาพที่ ๓.๘ แสดงขั้นตอนการ Get Report Process

๓.๕ การออกแบบการคำนวณค่า Risk Result

Risk Result เป็นค่าที่บ่งบอกถึงระดับความเสี่ยงของข้อมูลภัยคุกคาม เช่น หมายเลขไอพี โดเมน ยู อาร์แอล และค่าแฮช หลังจากที่ผ่านการวิเคราะห์ภัยคุกคามโดยผู้ให้บริการวิเคราะห์ภัยคุกคามออนไลน์จาก ๓ ผู้ให้บริการดังนี้

๓.๕.๑ IBM X-Force Exchange (IBM) เป็นแพลตฟอร์ม CTI ที่ถูก พัฒนาโดยบริษัท IBM เพื่อใช้สำหรับแลกเปลี่ยนข้อมูลภัยคุกคามที่เก็บรวบรวมข้อมูลภัยคุกคามระหว่าง IBM และผู้ใช้งานทั่วโลกผ่านระบบ IBM Cloud ที่เรียกว่า IBM X-Force Exchange ซึ่ง พัฒนาอยู่บนระบบความปลอดภัยอัจฉริยะขนาดใหญ่ของ IBM ที่รวบรวมเข้ากับฐานข้อมูลงานวิจัย เชิงลึกด้านภัยคุกคาม และเทคโนโลยี QRadar ซึ่งสนับสนุนโดยเครือข่ายของนักวิเคราะห์และผู้เชี่ยวชาญด้านความปลอดภัยจาก IBM Managed Security Services โดย X-Force Exchange

๓.๕.๒ Virus Total (VT) เป็นบริษัทแอนตี้ไวรัสที่ Google เป็นเจ้าของมาตั้งแต่ปี ๒๐๑๒ และย้ายเข้ามาอยู่ภายใต้ Chronicle ซึ่งเป็นบริษัททางด้านความปลอดภัยใหม่ในเครือ Alphabet เมื่อต้นปี ๒๐๑๘ ทั้งยังเป็นแหล่งรวบรวม Engines ของผลิตภัณฑ์ป้องกันไวรัสจำนวนมาก เพื่อให้บริการ Sandboxing ออนไลน์ผ่านเว็บไซต์ ซึ่งผู้ใช้สามารถอัปโหลดไฟล์หรือยูอาร์แอล ขึ้นไปตรวจสอบว่ามีมัลแวร์และภัยคุกคามอื่นๆ แฝงอยู่ด้วยหรือไม่โดยกดอัปโหลดได้ทันที นอกจากนี้ยังรองรับไฟล์ทุกประเภท ผลลัพธ์การสแกนไฟล์จะแสดงออกมาเป็นคะแนน โดยจะดึงผลจากผู้ให้บริการแอนตี้ไวรัสทั้งหมดมาแสดงผลให้กับผู้ใช้บริการ และมีเอพีไอในการเชื่อมต่อใช้งานอัตโนมัติ

๓.๕.๓ Hybrid Analysis (HA) เป็นระบบที่ให้บริการวิเคราะห์มัลแวร์ฟรีจาก CrowdStrike Falcon® Sandbox. ซึ่งให้บริการตรวจจับและวิเคราะห์ภัยคุกคามที่ไม่รู้จักโดยใช้เทคโนโลยี Hybrid Analysis ที่เป็น Sandboxing ออนไลน์ผ่านเว็บไซต์ สามารถอัปโหลดไฟล์ขึ้นไปสแกนได้ทันทีและรองรับไฟล์ทุกประเภท และรองรับการใช้งานเอพีไอในการเชื่อมต่ออัตโนมัติด้วยเช่นกัน

ค่า Risk Result จะเป็นค่าความเสี่ยงที่ถูกประเมินโดยผู้ให้บริการวิเคราะห์ภัยคุกคามออนไลน์จากทั้ง ๓ ผู้ให้บริการหลังจากที่ระบบส่งไฟล์ไปสแกน ซึ่งค่าที่ได้มานั้นจะมีความแตกต่างกัน และจะถูกคำนวณใหม่เพื่อแปลงค่าออกมาให้เป็นเปอร์เซ็นต์ ให้อยู่ในรูปแบบเดียวกันโดยใช้สูตรการคำนวณดังนี้

ตัวอย่างการคำนวณ

$$(x / n) * 100 = X\%$$

x = จำนวน Engines ของแอนตี้ไวรัสที่ตรวจพบว่าไฟล์ติดมัลแวร์

n = จำนวน Engines ของแอนตี้ไวรัสทั้งหมดทที่ใช้สแกนไฟล์

โดยเมื่อได้ค่าเปอร์เซ็นต์ออกมากแล้วจึงนำไปเทียบเกณฑ์ โดยใช้หลักเกณฑ์คือ High 100% Medium 60% Low 20% ตามลำดับ

๓.๖ การออกแบบการคำนวณค่า Confidence Level

ค่า Confidence Level เป็นค่าที่ได้จากการนำเอาค่า Risk Result จากทั้ง ๓ ผู้ให้บริการวิเคราะห์ภัยคุกคามออนไลน์มาแสดงเป็นผลรวม สำหรับเก็บค่าทางสถิติของภัยคุกคามนั้น และใช้เป็นส่วนประกอบในการนำข้อมูลภัยคุกคามนี้ไปใช้วิเคราะห์ร่วมกับหลักฐาน หรือเหตุการณ์อื่นเพิ่มเติมเพื่อใช้พิจารณาเหตุการณ์การโจมตีเครือข่ายที่เกิดขึ้น

บทที่ ๔
ผลการทดลองและการดำเนินงาน

๔.๑ อุปกรณ์และซอฟต์แวร์ที่ใช้ในการทำโครงงาน

๔.๑.๑ เครื่องคอมพิวเตอร์รุ่น Acer Predator Helios PH16-72-92WW

๔.๑.๒ เครื่องคอมพิวเตอร์รุ่น MacBook Pro 14

๔.๑.๓ ระบบ Front-End พัฒนาขึ้นด้วยภาษา PHP โดยใช้ Bootstrap เป็น Framework

๔.๑.๔ ระบบ Back-End พัฒนาขึ้นด้วยภาษา Python และ Shell Script

๔.๑.๕ ระบบฐานข้อมูลใช้ MySQL เป็นฐานข้อมูลและใช้ phpMyAdmin ในการบริหารจัดการ

๔.๑.๖ การติดตั้งระบบและเครือข่ายทั้งหมดติดตั้งบนระบบ Google Cloud Platform

๕.๑.๗ ซอฟต์แวร์ (Software)

- OS: CentOS7 Windows10
- NGINX 1.16.1
- pgp
- XAMPP3.2.4
- PHP 5.4.16
- Python3.7.4
- Visual Studio Code 1.39.2
- MySQLServer7
- phpMyAdmin 4.4.15.10
- Google Cloud Platform

๔.๒ ผลการพัฒนาระบบ

ในส่วนของการพัฒนาระบบต้นแบบจะทำงานอยู่บนฮาร์ดแวร์ที่ใช้ localhost โดยมีรายละเอียดดังนี้

๔.๒.๑ เครื่อง Front-End Server ทำหน้าที่เป็น Web Server ใช้ระบบปฏิบัติการ CentOS 7 และติดตั้งซอฟต์แวร์ NGINX ในการรัน Web Server

๔.๒.๒ เครื่อง Back-End Server ทำหน้าที่เป็นตัวกลางในการเชื่อมต่อกับระบบฐานข้อมูล เชื่อมต่อกับเอพีไอของระบบ Online Threat Intelligence, Online Threat Intelligence DB และเป็นเอพีไอที่ให้บริการกับระบบ Front-End ซึ่งจะใช้ระบบปฏิบัติการ Linux CentOS 7 ติดตั้งซอฟต์แวร์ Python และส่วนเสริม Flask, mod_wsgi เพื่อใช้สำหรับพัฒนาเอพีไอ

๔.๒.๓ เครื่อง Database Server ทำหน้าที่เป็นระบบฐานข้อมูลเพื่อจัดเก็บข้อมูล ที่ใช้ในการทำงานของระบบ ใช้ระบบปฏิบัติการ Linux CentOS 7 ติดตั้งซอฟต์แวร์ MySQL และ phpMyAdmin

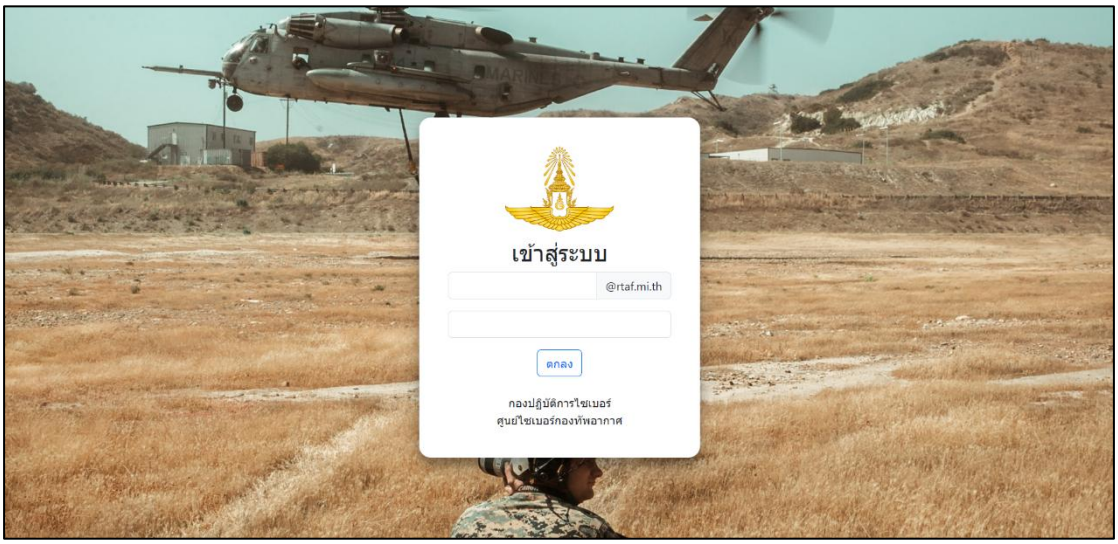
๔.๒.๔ เครื่องฮาร์แวร์ที่ใช้ในการพัฒนา Source Code ติดตั้งระบบปฏิบัติการ Windows10 ติดตั้งซอฟต์แวร์ XAMPP การรัน Web Server และติดตั้ง Visual Studio Code

๔.๓ ผลการดำเนินงาน

ผลการพัฒนาระบบวิเคราะห์ข้อมูลภัยคุกคามทางไซเบอร์ของกองทัพอากาศเป็นระบบวิเคราะห์ข้อมูลภัยคุกคามออนไลน์ และคำนวณระดับความเชื่อมั่นของผลการวิเคราะห์ข้อมูล เพื่อใช้เป็นส่วนช่วยในการตัดสินใจเกี่ยวกับภัยคุกคาม และสามารถค้นหาข้อมูลได้โดยตรงจากผู้ให้บริการวิเคราะห์ภัยคุกคามออนไลน์ผ่านทางหน้าเว็บไซต์ที่ให้บริการ จึงทำให้ผู้ใช้งานใช้เวลาในการค้นหาข้อมูลที่มีความเกี่ยวข้องกับภัยคุกคามที่ต้องการค้นหาสั้นลง โดยระบบในภาพรวมมีรายละเอียดดังต่อไปนี้

๔.๓.๑ หน้าแรกของระบบ

ผู้ใช้งานทำการ Login เข้าสู่ระบบโดยใช้อีเมลกองทัพอากาศพร้อมทั้งรหัสผ่านดังแสดงในภาพที่ ๔.๑

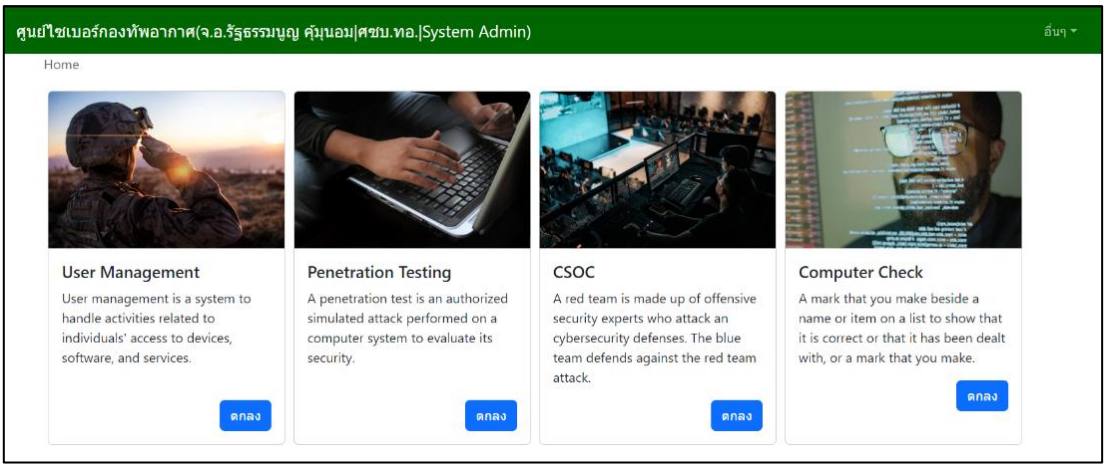


ภาพที่ ๔.๑ หน้า Login

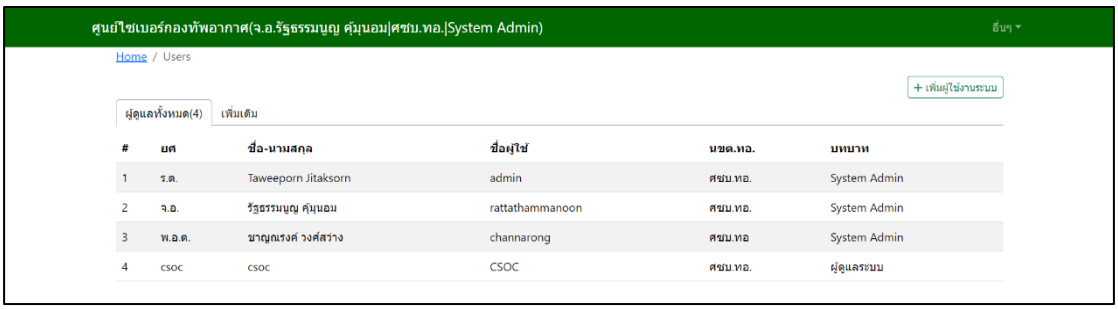
เมื่อผู้ใช้งานเข้าสู่ระบบแล้ว ระบบจะแสดงฟังก์ชันการทำงานต่าง ๆ ประกอบด้วย User Management, Penetration Testing, CSOC, Computer Check ดังแสดงในภาพที่ ๔.๒

๔.๓.๒ User Management

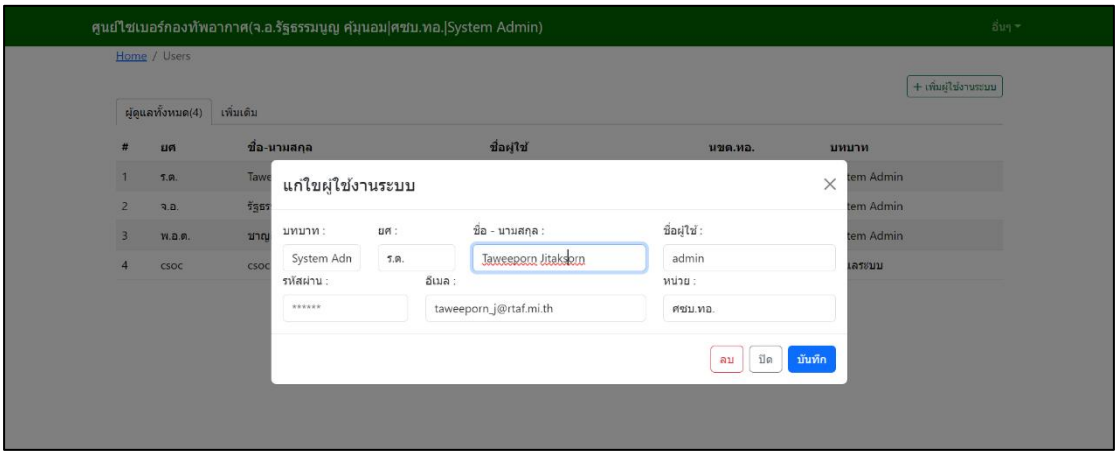
ฟังก์ชัน User Management ใช้ในการบริหารจัดการข้อมูลผู้ใช้งาน เช่น หน้าแสดงผู้จัดการระบบดังแสดงในภาพที่ ๔.๓ การแก้ไขรายละเอียดผู้ใช้งานระบบดังแสดงในภาพที่ ๔.๔ การเพิ่ม/ลบ ผู้ใช้งานในระบบดังแสดงในภาพที่ ๔.๕ - ๔.๗



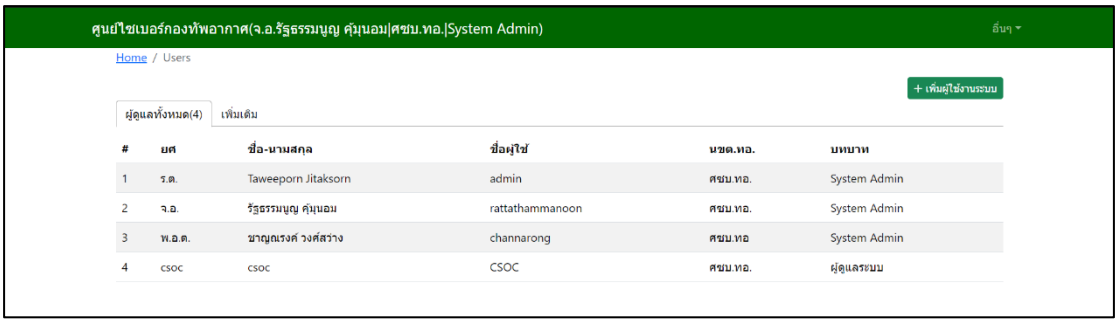
ภาพที่ ๔.๒ ระบบฟังก์ชันต่าง ๆ ของระบบ



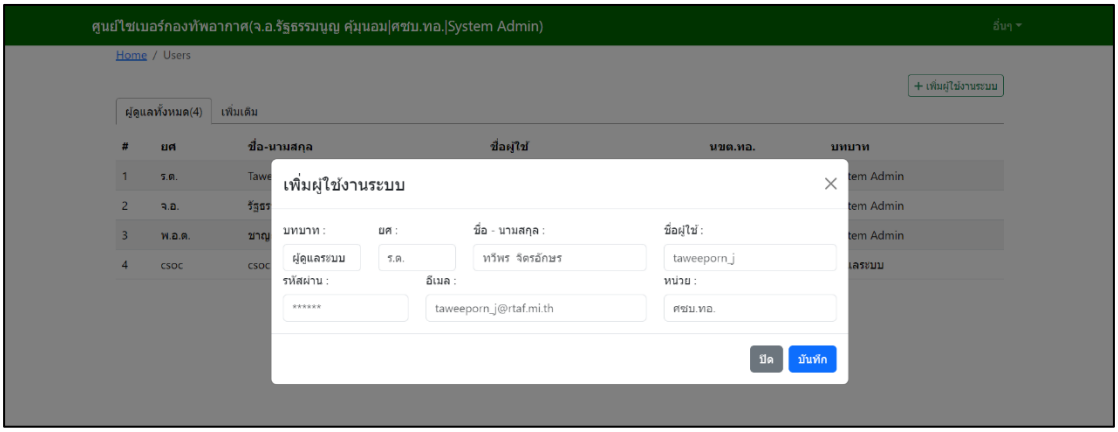
ภาพที่ ๔.๓ การแสดงผู้ดูแลทั้งหมด



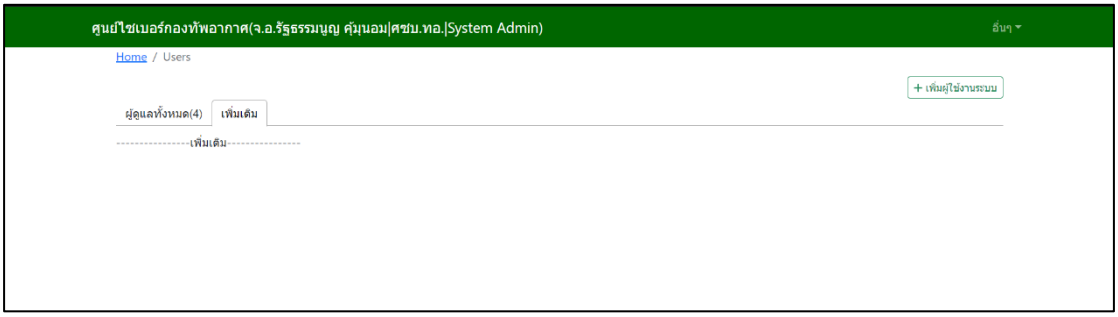
ภาพที่ ๔.๔ การแสดงหน้าการแก้ไขผู้ใช้งานระบบ (การแก้ไขชื่อผู้ใช้งาน)



ภาพที่ ๔.๕ การแสดงหน้าการแก้ไขผู้ใช้งานระบบ (การเพิ่มผู้ใช้งานระบบ - ๑)



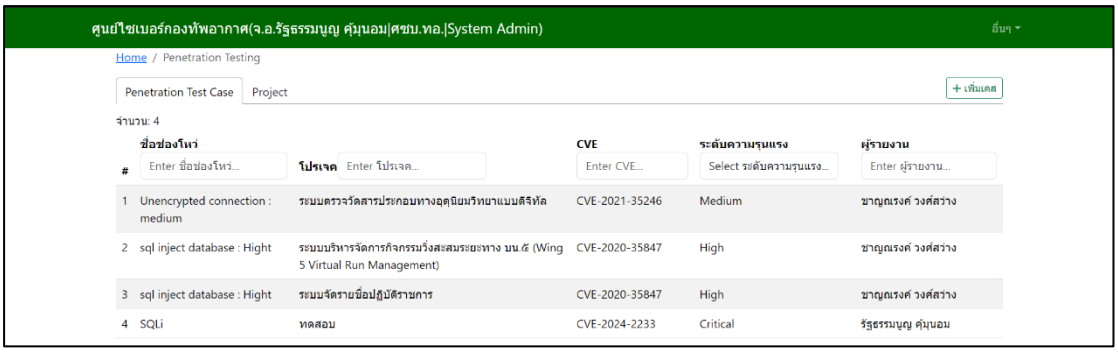
ภาพที่ ๔.๖ การแสดงหน้าการแก้ไขผู้ใช้งานระบบ (การเพิ่มผู้ใช้งานระบบ - ๒)



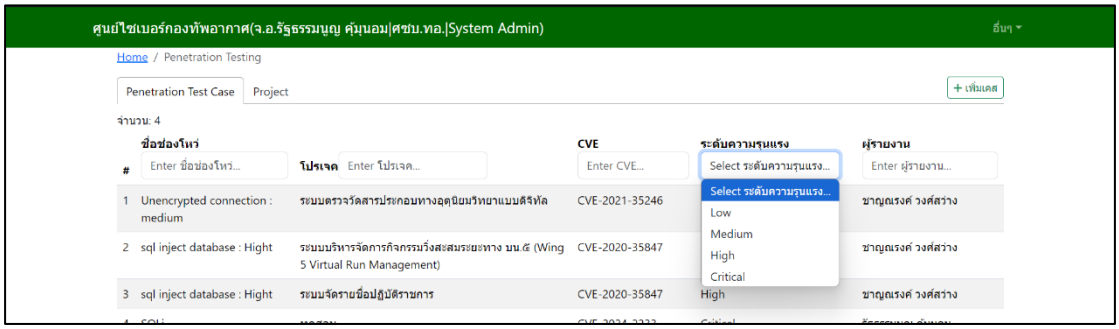
ภาพที่ ๔.๗ การแสดงหน้าการแก้ไขผู้ใช้งานระบบ (การเพิ่มผู้ใช้งานระบบ - ๓)

๔.๓.๓ Penetration Testing Case

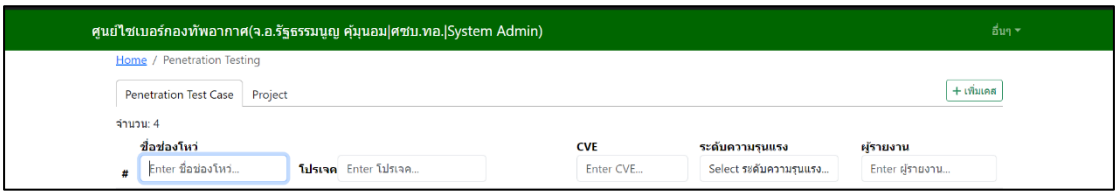
ฟังก์ชัน Penetration Testing Case เป็นหน้าจัดการผลการทดสอบระบบความมั่นคงปลอดภัยเพื่อใช้เป็นข้อมูลในการเฝ้าระวังภัยคุกคามทางไซเบอร์จากเหตุการณ์ (Incidents) ที่เกิดขึ้นพร้อมทั้งระดับ CVE และความรุนแรง รวมถึงผู้รายงานเหตุการณ์ โดยผู้ใช้งานสามารถเพิ่ม/ลบ แก้ไข ภัยคุกคามรวมถึงการมอบหมายหน่วยงานรับผิดชอบได้ ดังแสดงในภาพที่ ๔.๘ - ๔.๑๓



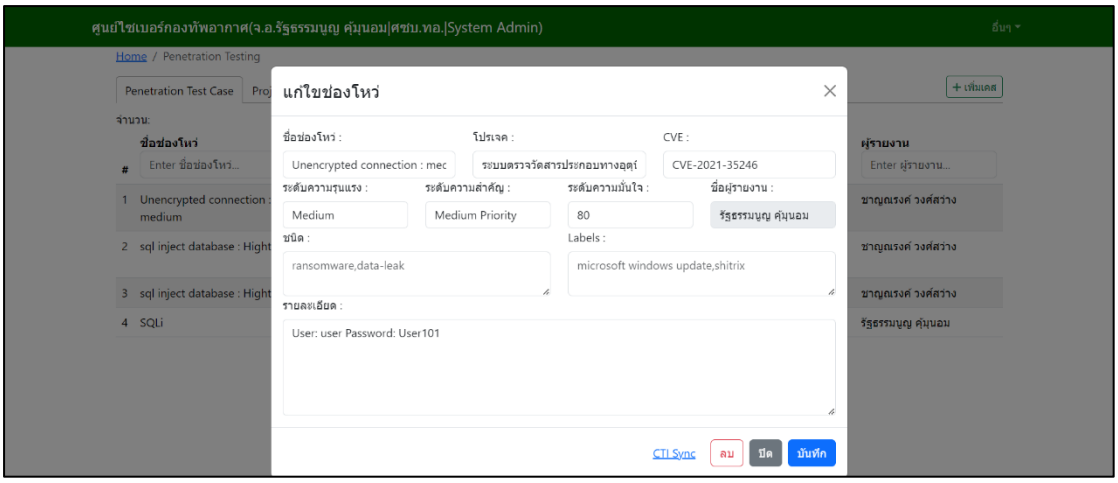
ภาพที่ ๔.๘ การแสดงหน้า Penetration Testing Case (ภาพรวม)



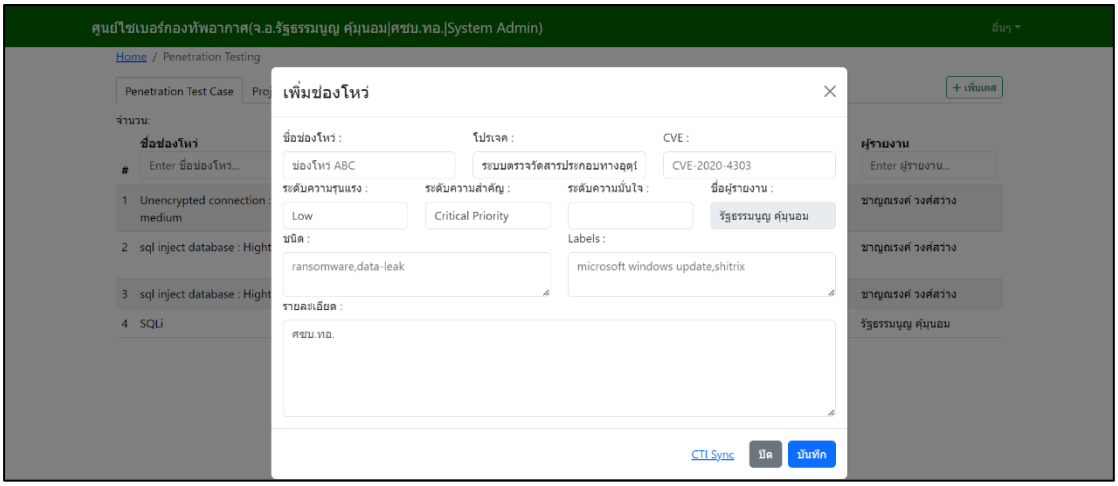
ภาพที่ ๔.๙ การแสดงหน้า Penetration Testing Case (ระดับความรุนแรง)



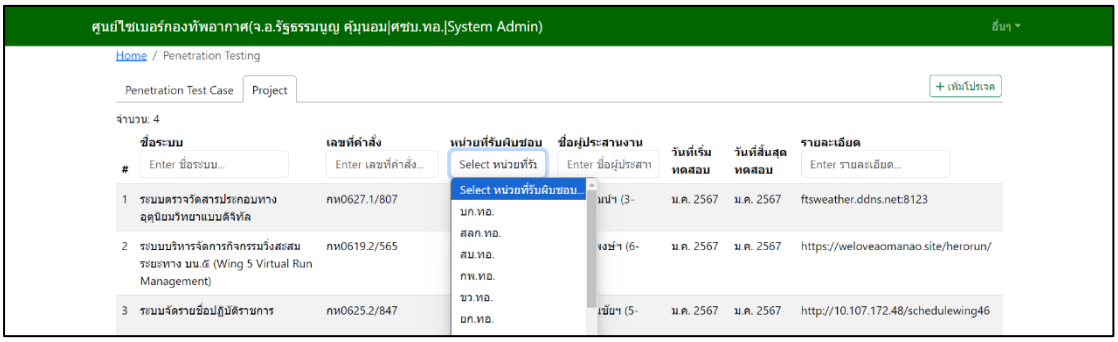
ภาพที่ ๔.๑๐ การแสดงหน้า Penetration Testing Case (การเพิ่มชื่อช่องโหว่)



ภาพที่ ๔.๑๑ การแสดงหน้า Penetration Testing Case (การแก้ไขช่องโหว่)



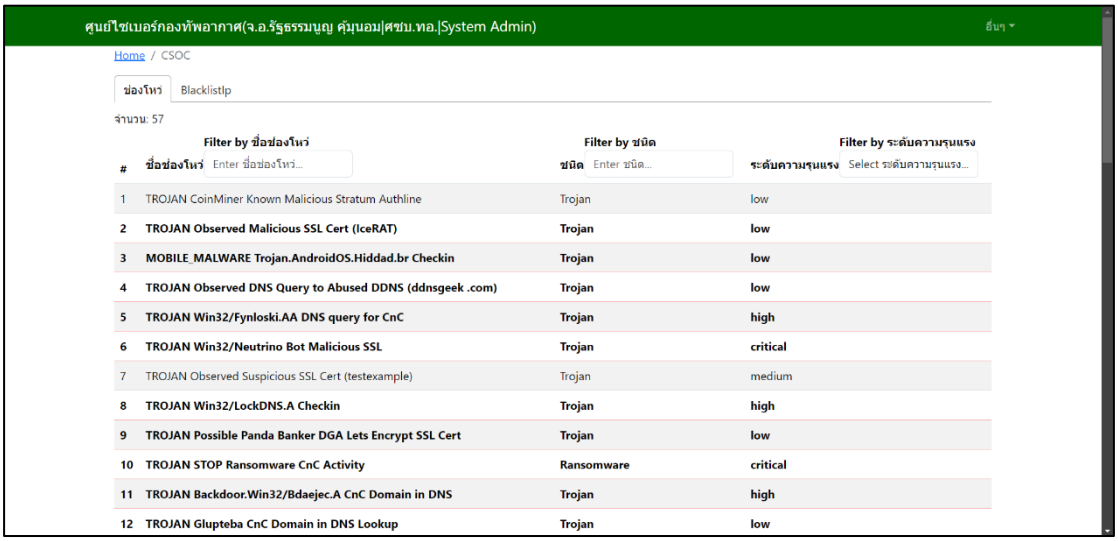
ภาพที่ ๔.๑๒ การแสดงหน้า Penetration Testing Case (การเพิ่มช่องโหว่)



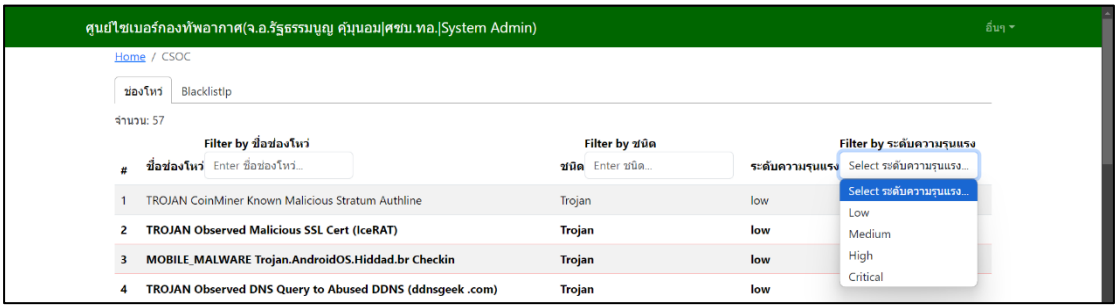
ภาพที่ ๔.๑๓ การแสดงหน้า Penetration Testing Case (การกำหนดหน่วยรับผิดชอบ)

๔.๓.๔ CSOC

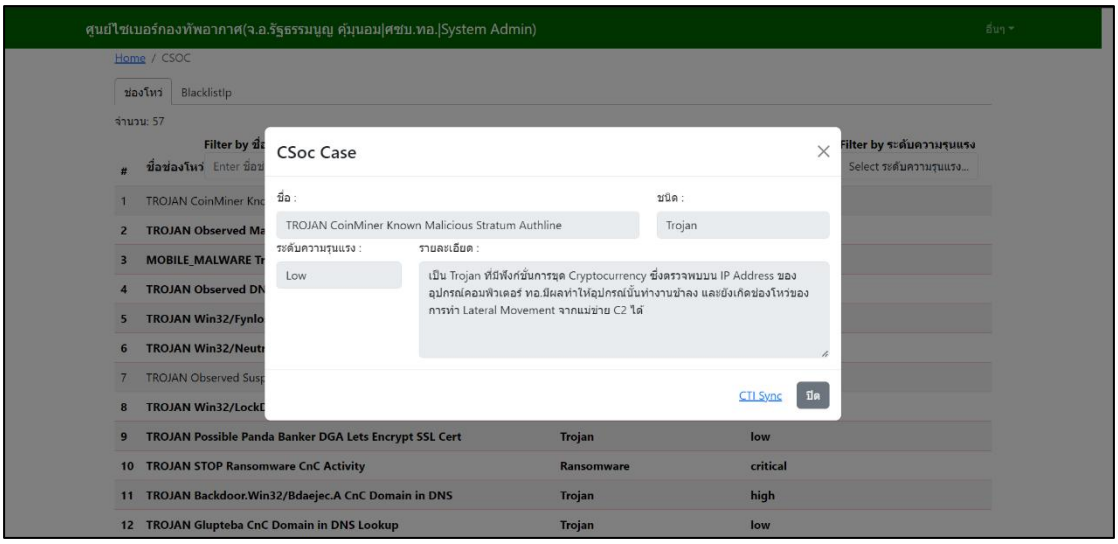
ฟังก์ชัน CSOC ใช้สำหรับศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งทำหน้าที่ตรวจจับ วิเคราะห์ รับมือ และจัดการภัยคุกคามทางไซเบอร์แบบเรียลไทม์ โดยมีทีมงานผู้เชี่ยวชาญและเทคโนโลยีที่ทันสมัยในการเฝ้าระวังข้อมูลเครือข่าย ระบบไอที และตอบสนองต่อเหตุการณ์ที่ไม่ปกติ เป้าหมายหลักคือปกป้องข้อมูล และระบบต่าง ๆ จากการโจมตีทางไซเบอร์ เช่น Malware, Phishing หรือการเจาะระบบ เพื่อรักษาความปลอดภัยและความน่าเชื่อถือขององค์กร สำหรับโดยสามารถใช้งานผ่านระบบ โดยสามารถค้นหาข้อมูลได้ด้วย เช่น หมายเลขไอพี โดเมน ยูอาร์แอล ค่าแฮช และการกรองข้อมูล (Filtering) เช่น การกรองผ่านชื่อการโจมตี ชนิดการโจมตี หรือระดับความรุนแรงของการโจมตี เพื่อให้ผลหน้าเว็บที่มีประสิทธิภาพมากขึ้นดังแสดงในภาพที่ ๔.๑๔ - ๔.๑๙



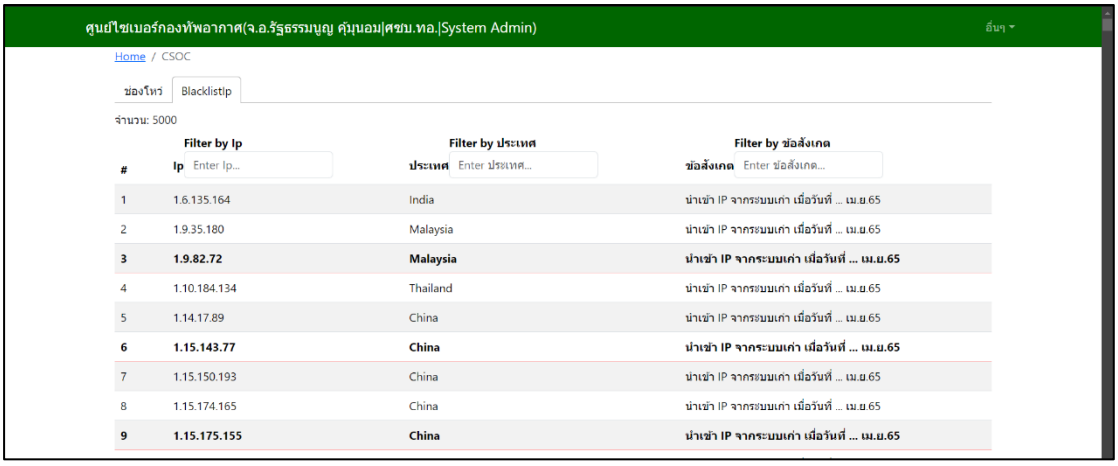
ภาพที่ ๔.๑๔ การแสดงภาพหน้า CSOC



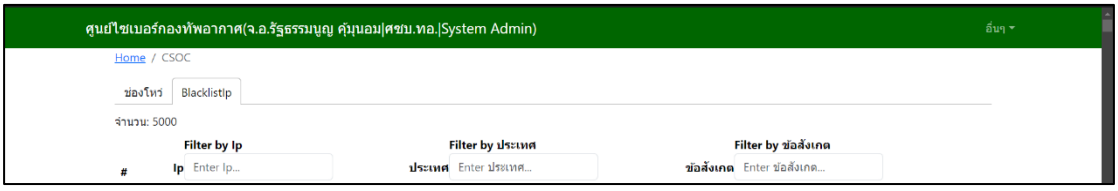
ภาพที่ ๔.๑๕ การปรับแต่งการแสดงผล (ระดับความรุนแรง)



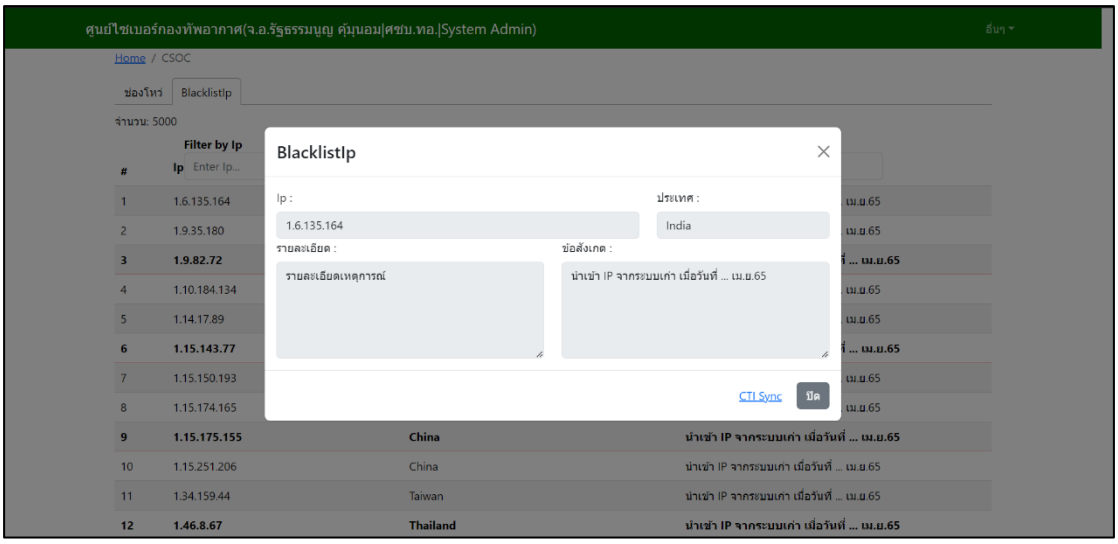
ภาพที่ ๔.๑๖ การแสดงรายละเอียด CSOC Case



ภาพที่ ๔.๑๗ การแสดงผลหมายเลข IP ของการโจมตี



ภาพที่ ๔.๑๘ การแสดงรายละเอียดการคัดกรองหมายเลขไอพีที่ต้องการ

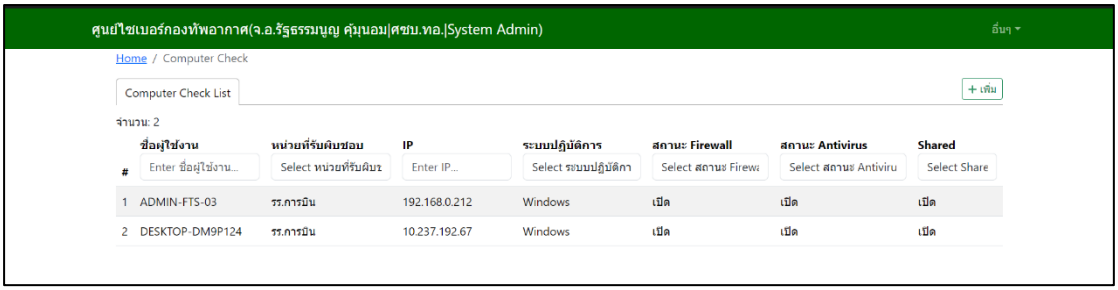


ภาพที่ ๔.๑๙ การแสดงรายละเอียด Blacklist IP

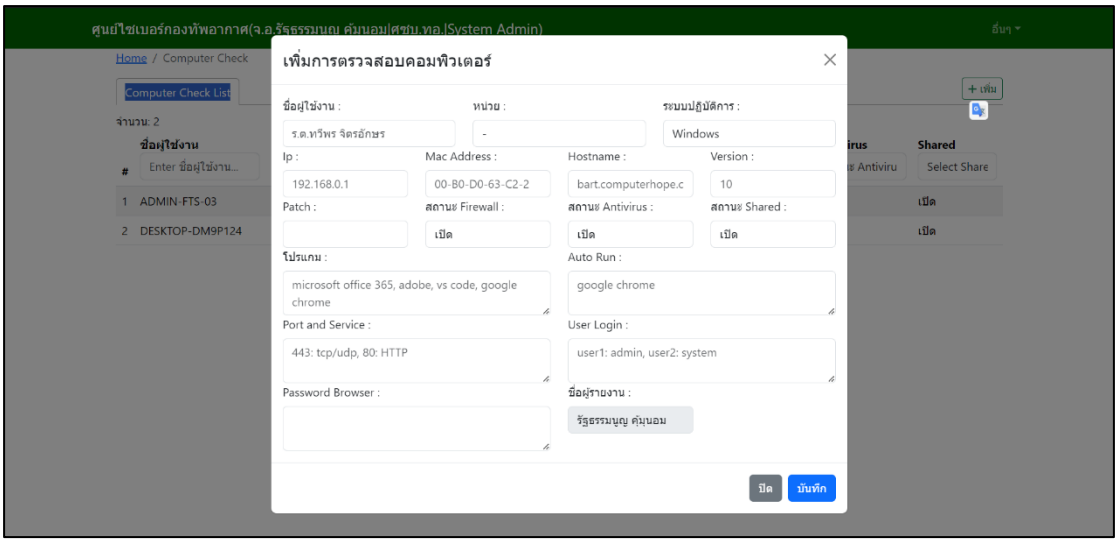
การใช้งานระบบยังสามารถแสดงรายละเอียดของข้อมูลภัยคุกคาม โดยแสดงผลรายงานการวิเคราะห์ข้อมูลภัยคุกคามที่ระบบส่งไปวิเคราะห์ยังผู้ให้บริการวิเคราะห์ภัย คุกคามออนไลน์ครั้งล่าสุด ๒๐ อันดับ ซึ่งได้แก่ข้อมูล Last Scan, Threat, Malware, Status, Host, ยูอาร์แอล, หมายเลขไอพี และค่าแฮช, Status, Actor Group และค่า Risk Result ที่ได้จากผลการ สแกนแยกตามผู้ให้บริการวิเคราะห์ภัยคุกคามออนไลน์ และ Confident Level ผ่านระดับความรุนแรง ดังรูปที่ ๔.๑๔ - ๔.๑๕

๔.๓.๕ Computer Check

ฟังก์ชันดังกล่าว ช่วยให้ผู้ดูแลระบบสามารถกำหนดเครื่องคอมพิวเตอร์ภายในองค์กรเพื่อเฝ้าระวังภัยคุกคาม พร้อมทั้งรายละเอียดสถานะด้านการป้องกันที่เกี่ยวข้องเช่น ชื่อผู้ใช้งาน หน่วยงานที่รับผิดชอบ หมายเลขไอพี ระบบปฏิบัติการที่กำลังใช้งาน สถานะของ Firewall/Antivirus รวมถึงสถานการณ์แชร์ข้อมูลของเครื่องคอมพิวเตอร์ดังแสดงในภาพที่ ๔.๒๐ - ๔.๒๑



ภาพที่ ๔.๒๐ การแสดงรายละเอียดระบบ Computer Check



ภาพที่ ๔.๒๑ การเพิ่มการตรวจสอบคอมพิวเตอร์

จากที่กล่าวมาทั้งหมดจะเห็นว่า ผู้วิจัยได้พัฒนาระบบวิเคราะห์ข้อมูลภัยคุกคามทางไซเบอร์ของกองทัพอากาศที่สามารถวิเคราะห์ข้อมูลภัยคุกคามออนไลน์ และคำนวณระดับความเชื่อมั่นของผลการวิเคราะห์ข้อมูล เพื่อใช้เป็นส่วนช่วยในการตัดสินใจเกี่ยวกับภัยคุกคาม และสามารถค้นหาข้อมูลได้โดยตรงจากผู้ให้บริการ วิเคราะห์ภัยคุกคามออนไลน์ผ่านทางหน้าเว็บไซต์ที่ให้บริการ จึงทำให้ผู้ใช้งานใช้เวลาในการค้นหาข้อมูลที่มีความเกี่ยวข้องกับภัยคุกคามที่ต้องการค้นหาสั้นลง และสามารถดำเนินการเพื่อป้องกันและแก้ไขภัยคุกคามต่อความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศได้อย่างทันท่วงที

บทที่ ๕
สรุปผลการดำเนินการ

๕.๑ ระบบวิเคราะห์ข้อมูลภัยคุกคามทางไซเบอร์

จากผลการวิจัยสรุปว่า ผู้วิจัยสามารถพัฒนาระบบวิเคราะห์ข้อมูลภัยคุกคามทางไซเบอร์เป็นระบบเปิดที่ให้บริการในการค้นหาข้อมูลภัยคุกคามทางไซเบอร์จากแหล่งผู้ให้บริการ Online Cyber Threat Intelligence จาก ๓ แหล่งที่มาพร้อมกันประกอบด้วย

๕.๑.๑ Virus Total (https://www.virustotal.com/) ซึ่งเป็นเว็บไซต์ของผู้ให้บริการ Online Cyber Threat Intelligence ที่ถูกพัฒนาขึ้นโดย Google Inc. ตั้งแต่เดือน มิ.ย. ๒๐๐๔ มีทีมนักวิจัยเกี่ยวกับภัยคุกคามและชุมชนนักปฏิบัติ (Community) คอยอัปเดตข้อมูลอย่างต่อเนื่องและเป็นเว็บไซต์ที่มี Antivirus Engines จำนวนมากที่คอยให้บริการวิเคราะห์ภัยคุกคาม จึงเป็นเว็บไซต์ที่นิยมใช้งานวิเคราะห์เกี่ยวกับภัยคุกคามทางไซเบอร์

๕.๑.๒ IBM® X-Force Exchange (https://exchange.xforce.ibmcloud.com/) เป็นเว็บไซต์ของผู้ให้บริการ Online Threat Intelligence Agency ที่ถูกพัฒนาขึ้นโดยบริษัท ไอบีเอ็ม ซึ่งเป็นผู้ให้บริการโซลูชันทางด้านเครือข่ายและความปลอดภัยที่มีชื่อเสียงและมีระบบ AI เข้ามาช่วยในการวิเคราะห์ภัยคุกคาม จึงเป็นเว็บไซต์ที่นักวิเคราะห์ภัยคุกคามให้ความเชื่อถือและเป็นที่นิยมเช่นกัน

๕.๑.๓ Hybrid Analysis (https://www.hybrid-analysis.com/) เป็นเว็บไซต์ของผู้ให้บริการ Online Cyber Threat Intelligence ที่มีความเชี่ยวชาญทางด้าน Sandbox ที่ถูกพัฒนาขึ้นโดย CrowdStrike Falcon ผู้ให้บริการโซลูชันด้านความปลอดภัยทางด้าน Endpoint Security และ Endpoint detection and Respond (EDR) ตรวจสอบลึกถึงกระบวนการ ในการทำงานของเครื่อง Endpoint ในการวิเคราะห์ภัยคุกคาม ทั้งยังเชื่อมต่อกับระบบคลาวด์จึงทำให้สามารถตรวจสอบและเฝ้าระวังภัยคุกคามได้จากทุกที่ที่มีการเชื่อมต่อกับอินเทอร์เน็ตเพียงแค่มีการติดตั้ง Agent ลงที่เครื่องอุปกรณ์ที่จะเฝ้าระวัง นั่นจึงเป็นจุดเด่นที่ทำให้ Hybrid-Analysis ถูกนำมาใช้ในการ ทดสอบระบบครั้งนี้

โดยระดับดังกล่าวสามารถตอบโจทย์เรื่องการลดเวลาในการค้นหาข้อมูลภัยคุกคามในงานวิเคราะห์ภัย คุกคามทางไซเบอร์ นอกจากระบบที่ได้พัฒนาขึ้นแล้ว ผู้ใช้งานสามารถใช้งานผ่านการเชื่อมต่อกับเอ พีไอได้อีกหนึ่งช่องทางเช่นกัน

๕.๒ ปัญหาและอุปสรรคในการดำเนินการ

๕.๒.๑ เรื่องของความเชื่อมั่น (Trust) ของข้อมูลที่นำมาใช้งาน แม้จะมีการส่งไปสแกนผลจากผู้ให้บริการ Online Threat Intelligence จากหลายที่แล้วก็ตาม อย่างไรก็ตามผู้ให้บริการแต่ละแหล่งข้อมูลมีการเก็บข้อมูลและการอัปเดตข้อมูลที่แตกต่างกัน ซึ่งอาจจะช้าหรือเร็วแตกต่างกัน เนื่องจากผลรายงานการสแกนที่ได้มานั้นเป็นเพียงส่วนหนึ่งที่จะช่วยในการตัดสินใจของนักวิเคราะห์ภัยคุกคามเท่านั้น และก็ยังต้องนำผลเหล่านี้ไปพิสูจน์ตรวจสอบและการเชื่อมโยงเหตุการณ์จากอีกหลายเหตุการณ์ประกอบกัน และยังจำเป็นที่ต้องใช้เวลาและทรัพยากรในการวิเคราะห์เช่นกัน

โดยเฉพาะปัจจุบันที่เทคนิคการหลบเลี่ยงการ ตรวจจับความปลอดภัยของกลุ่มแฮกเกอร์นั้นสูงขึ้น ส่งผลให้ภัยคุกคามบางประเภทแฝงตัวซ่อนอยู่ในเครือข่ายนานหลายปีจึงสามารถตรวจจับได้

๕.๒.๒ การเลือกใช้ผู้ให้บริการ Online Cyber Threat Intelligence ซึ่งแต่ละแหล่งข้อมูลมีความชำนาญในการวิเคราะห์ภัยคุกคามที่ต่างกัน ผลรายงานจากการสแกนหากมีการนำไปใช้เพื่อคำนวณหาค่าความเสี่ยงของภัยคุกคามหรือระดับความเชื่อมั่นจะทำได้ยากและมีโอกาสที่ผลจะคลาดเคลื่อนและโอกาสเกิด False Positive สูง

๕.๒.๓ ข้อจำกัดด้านโควตาในการนำข้อมูลไปสแกนยังผู้ให้บริการ Online Cyber Threat Intelligence แต่ละที่จะมีโควตาที่จำกัดทำให้ไม่สามารถนำข้อมูลที่มีในระบบส่งไปสแกนเพื่อวิเคราะห์ ภัยคุกคามได้แบบ Real-Time และข้อมูลอาจจะไม่อัปเดตได้เท่าที่ควรเนื่องจากข้อมูลในระบบ นั้นมีข้อมูลจำนวนมาก

๕.๒.๔ ความแตกต่างระหว่างรูปแบบธุรกิจของผู้ให้บริการ เนื่องจากรูปแบบธุรกิจของแต่ละองค์กรนั้นแตกต่างกัน ความเสี่ยงย่อมแตกต่างกัน ข้อมูลที่ได้มานั้นมีปริมาณที่มากกว่าความต้องการที่จะนำมาใช้งานจริง การกรองข้อมูลนั้นจึงต้องใช้ ทรัพยากรจำนวนมากในการจัดการ

๕.๒.๕ ผู้ให้บริการ Online Cyber Threat Intelligence ที่เปิดให้ใช้งานวิเคราะห์ภัยคุกคาม ผ่านการเชื่อมต่อเอพีไอในการส่งข้อมูลไปวิเคราะห์โดยไม่มีค่าใช้จ่ายในการใช้บริการนั้นยังมีจำนวนจำกัด และส่วนมากจะเสียค่าบริการรายเดือนและค่าใช้จ่ายค่อนข้างสูง

๕.๓ ข้อเสนอแนะ

๕.๓.๑ ปรับปรุงให้สามารถเพิ่มฟังก์ชันคอมเมนต์ Event Data เหตุการณ์หรือข้อมูลภัยคุกคามและแหล่งข้อมูลต้นทาง (Source Feeds) ที่จะดึงข้อมูลภัยคุกคามผ่านทางหน้าเว็บไซต์ได้

๕.๓.๒ เพิ่มการให้คะแนนความเชื่อมั่นผ่านหน้าเว็บไซต์แล้วคำนวณออกมาเป็นค่าความ พึงพอใจจากการใช้งานข้อมูล

๕.๓.๓ เพิ่มความสามารถในการตรวจสอบกับข้อมูล CVE (Common Vulnerabilities and Exposures) ซึ่งเป็นข้อมูลช่องโหว่ที่ถูกค้นพบของระบบปฏิบัติการต่าง ๆ ได้และถูกเปิดเผยเป็นสาธารณะ

๕.๓.๔ เพิ่มความสามารถในการเชื่อมต่อกับระบบอื่นแบบอัตโนมัติ

๕.๓.๕ เพิ่มฟังก์ชันในการคำนวณค่าความเสี่ยงเมื่อข้อมูลภัยคุกคามนั้นมีเหตุการณ์ที่เชื่อมโยงกับระบบที่มีผลกระทบสูง

บรรณานุกรม

ภาษาไทย

พงษ์สวัสดิ์ จ. (๒๕๖๑). *การพัฒนางานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร*

ทองม่วง, น. (๒๕๖๓). *แนวทางการพัฒนาระบบงานด้านข่าวกรองด้วยเทคโนโลยีสารสนเทศ กองข่าว กองทัพภาคที่ ๑*. สถาบันวิชาการป้องกันประเทศ. https://awc.ac.th/storage/research/436.pdf

สหรัฐฯ ประกาศภาวะฉุกเฉินหลัง บ.ท่อส่งน้ำมันรายใหญ่โดนมัลแวร์เรียกค่าไถ่โจมตี, สืบค้นเมื่อ ๒๕๖๕. https://www.bbc.com/thai/international-57052951

แฮคโรงพยาบาล-รีดค่าไถ่ เรียกถึง 6.3 หมื่นล้านบาท, ๑๐ ก.ย. ๒๕๖๓, สืบค้นเมื่อ ๒๕๖๕ https://www.thairath.co.th/news/local/central/1926912

สรุปผลการตรวจสอบเหตุการณ์ข้อมูล Username/Password ทอ.รั่วไหล”(๒๕๖๓).

“หลักนิยมการปฏิบัติการไซเบอร์” กองทัพอากาศ (๒๕๖๓).

“พบเกาหลีเหนืออาจพัวพันเหตุมัลแวร์โจมตีทั่วโลก”. (๒๕๖๐)**.** สืบค้นเมื่อ ๒๕๖๕**,** https://www.bbc.com/thai/international-39931940

Microsoft. (n.d.). *ข่าวกรองภัยคุกคามไซเบอร์คืออะไร*. Retrieved from https://www.microsoft.com

SANS Institute. (2022, January 20). *ความรู้พื้นฐานเกี่ยวกับภัยคุกคามทางไซเบอร์: ปลดล็อคเทคโนโลยีทรงพลัง!*. Retrieved from https://www.sans.org

สำนักข่าวกรองแห่งชาติ. (n.d.). *ภัยคุกคามทางไซเบอร์ ๕ ประเด็น ที่ควรเฝ้าติดตามในปี ๒๕๖๕*. Retrieved from https://www.nia.go.th

ภาษาอังกฤษ

Perkins, D. (2023). The evolution of intelligence: Analysis of the Journal of Intelligence and Intelligence (2013–2022). *Journal of Intelligence*, 11(2), 35.

Centre for the Protection of National Infrastructure, & MWR InfoSecurity. (2015). *Threat intelligence: Collecting, analyzing, evaluating*. https://www.foo.be/docs/informations-sharing/Threat-Intelligence-Whitepaper.pdf

Central Intelligence Agency. (2023). *The IC OSINT strategy 2024-2026*. https://www.cia.gov/static/9d89dd9a4fe41b63cfab00c5191a8803/IC-OSINT-Strategy.pdf

National Cyber Security Centre. (2014). *An introduction to threat intelligence*. National Cyber Security Centre. Retrieved December 2, 2024, from https://www.ncsc.gov.uk/files/An-introduction-to-threat-intelligence.pdf

Marr, B. (2020). *Big Data in Practice: How 45 Successful Companies Used Big Data Analytics to Deliver Extraordinary Results*. Wiley.

Microsoft. (n.d.). *Cybersecurity Threat Intelligence and Big Data Challenges*. Retrieved from https://www.microsoft.com

Kaspersky. (n.d.). *Indicators of Compromise: Definition and Examples*. Retrieved from https://www.kaspersky.com

Symantec. (n.d.). *What Are Indicators of Compromise (IoC)?* Retrieved from https://www.symantec.com

SANS Institute. (2019). *The Importance of Indicators of Compromise in Cybersecurity Operations*. Retrieved from https://www.sans.org

MFEC. (n.d.). *Incident Response & Forensics: สิ่งที่ต้องรู้ในยุคไซเบอร์*. Retrieved from mfec.co.th

Microsoft. (n.d.). *What Are Indicators of Compromise (IoC)?*. Retrieved from https://www.microsoft.com

SentinelOne. (n.d.). *What Are Indicators of Compromise (IoCs)? A Comprehensive Guide*. Retrieved from https://sentinelone.com

Bianco, D. (2013). *The Pyramid of Pain*. Retrieved from detect-respond.blogspot.com

SANS Institute. (2020). *Using IoCs and Pyramid of Pain in Threat Hunting*. Retrieved from https://www.sans.org

Deloitte. (2021). *Cyber Risk Management: A Practical Approach*. Retrieved from https://www2.deloitte.com/

International Organization for Standardization. (2018). *ISO/IEC 27005: Information security risk management*.

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1). Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology. (2020). *Integrating Cybersecurity and Enterprise Risk Management (ERM)*. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf

UpGuard. (2023). *How to Perform a Cyber Risk Analysis*. Retrieved from https://www.upguard.com/blog/how-to-perform-a-cyber-risk-analysis

Alhazmi, O. H., & Malaiya, Y. K. (2014). *Threat intelligence and the role of Python in cybersecurity*. IEEE Security & Privacy.

Casey, E. (2015). *The use of Python in digital forensics and cybersecurity*. Digital Investigation Journal.

Python Software Foundation. (2023). *Python documentation*. Retrieved from https://www.python.org/doc/

SANS Institute. (2020). *Python for cybersecurity: A beginner's guide*. Retrieved from https://www.sans.org/

Schneider, M. (2017). *Malware analysis using Python*. Wiley Cybersecurity Series.

Sharma, A. (2020). *MERN Stack Development: The Complete Guide*. O'Reilly Media.

Kumar, S. (2019). *Cybersecurity Applications Using MERN Stack*. Springer International Publishing.

Cohen, D., & Stump, L. (2022). *Threat Intelligence Sharing with MISP*. Cybersecurity Journal, 14(2), 45-50.

David, M. (2021). *Analyzing Cyber Threats Using MISP*. ACM Security Conference Proceedings.

MISP Project. (2023). *MISP: Malware Information Sharing Platform*. Retrieved from https://www.misp-project.org

Wagner, C., Dulaunoy, A., & Iklody, A. (2020). *Practical Applications of MISP in Threat Intelligence Sharing*. Threat Intelligence Quarterly, 8(3), 20-30.

Bouchet, M., Bringer, J., Caumes, A., & Puys, M. (2021). *Enhancing Cyber Threat Intelligence Analysis Using OpenCTI*. Journal of Cybersecurity, 10(3), 45-60.

OpenCTI Documentation. (2023). *OpenCTI: Open Cyber Threat Intelligence Platform*. Retrieved from https://docs.opencti.io/latest/

OpenCTI-Platform. (2023). *OpenCTI Knowledge Graph Examples*. Retrieved from https://github.com/OpenCTI-Platform/opencti

“Joint Publication 3-12 cyberspace operations”, (2018). accessed 2021, Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/.

“Joint Publication 2-0 joint intelligence”, (2013). accessed 2021, Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf

“SCOTT JASPER. (2020) “RUSSIAN CYBER OPERATIONS”

“Cyber Security”. accessed 2021, Retrieved from https://www.rdpb.go.th/MediaUploader/File/10166/CyberSecurity

ผนวก ก คำจำกัดความ

คำจำกัดความด้านไซเบอร์

เพื่อให้เกิดความเข้าใจในแนวทางที่สอดคล้องกัน และเพื่อความสะดวกในการอ้างอิงสำหรับการศึกษาและใช้เป็นกรอบในการดำเนินการด้านสงครามไซเบอร์ของ ทอ. จึงได้กำหนดคำจำกัดความหรือคำนิยามศัพท์ด้านไซเบอร์ดังนี้

๑. การกระทำโดยรัฐ (State Actor) หมายถึง การปฏิบัติในมิติไซเบอร์ใบลักษณะที่เป็นภัยคุกคามโดยมีรัฐให้การสนับสนุนหรือสั่งการ

๒. การกระทำที่มิได้ดำเนินการโดยรัฐ (Non-state Actor) หมายถึง การปฏิบัติในลักษณะที่เป็นภัยคุกคาม โดยปราศจากการสนับสนุนหรือสั่งการจากรัฐ

๓. การตรวจสอบความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Audit) หมายถึง การตรวจสอบการปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยไม่กำหนดวิธีการหรือขั้นตอนที่จะดำเนินการตรวจสอบ เพื่อให้ได้ผลการตรวจสอบตามความเป็นจริง

๔. การโจมตีทางไซเบอร์ (Cyber Attack) หมายถึง การโจมตีต่อฝ่ายตรงข้ามโดยมีวัตถุประสงค์เพื่อขัดขวาง (Disrupt) ทำลาย (Destroy) หรือควบคุม (Control) การใช้งานมิติไซเบอร์ของฝ่ายตรงข้ามรวมถึงการทำลาย เปลี่ยนแปลง หรือขโมยข้อมูลของฝ่ายตรงข้ามด้วย

๕. การทำให้ระบบเป้าหมายปฏิเสธหรือหยุดการให้บริการ (Distributed Denial of Service: DDoS) หมายถึง การขัดขวางหรือก่อกวนระบบเครือข่ายหรือ Server จนทำให้ทรัพยากรของเครื่องเป้าหมายที่ถูกโจมตีหมดไป หรือเครือข่ายนั้น ๆ ไม่สามารถทำงานได้ตามปกติ

๖. การรับรองความสามารถด้านไซเบอร์ทางทหาร (Cyber Defense Certification) หมายถึง ระบบการพัฒนาขีดความสามารถของนักรบไซเบอร์ ประกอบด้วยการทดสอบความสามารถทางไซเบอร์ด้านทฤษฎีและปฏิบัติ ซึ่งจำเป็นต่อการปฏิบัติงานในมิติไซเบอร์ โดยแบ่งเป็นระดับที่แตกต่างกันตามขอบเขตความรับผิดชอบและลักษณะงาน เพื่อให้กระทรวงกลาโหมมีนักรบไซเบอร์ที่เพียงพอทั้งในเชิงปริมาณและเชิงคุณภาพ ตามมาตรฐานของกระทรวงกลาโหม

๗. การหลอกลวงทางอินเทอร์เน็ต (Phishing) หมายถึง การล่อลวงทางอินเทอร์เน็ตชนิดหนึ่ง ที่พยายามหลอกผู้ใช้งาน โดยการสร้างอีเมล หรือหน้าเว็บไซต์ปลอมขึ้นมาเพื่อหวังผลในการให้ผู้ใช้งานเกิดความสับสน และทำธุรกรรมต่าง ๆ บนเว็บไซต์ปลอมที่ถูกสร้างขึ้นนั้น โดยข้อมูลต่าง ๆ ที่ผู้ใช้งานได้กรอกบนหน้าเว็บไซต์ปลอมเหล่านี้ จะถูกดักข้อมูลและบันทึกไว้เพื่อใช้ในการปลอมแปลงและเข้าถึงข้อมูลของผู้เสียหายโดยที่ไม่ได้รับอนุญาต ส่วนการหลอกลวงแบบเจาะจงเป้าหมาย (Spear Phishing) คือ รูปแบบการหลอกลวงของข้อความอีเมลที่เฉพาะเจาะจง ซึ่งอาจดูเสมือนว่านายจ้างหรือเพื่อนร่วมงานส่งข้อความอีเมลให้คนในองค์กร

๘. การสืบสวนทางไซเบอร์ (Cyber Forensics/Computer Forensics) หมายถึง กระบวนการสกัดข้อมูลข่าวสารจากคอมพิวเตอร์และสื่อบันทึกข้อมูลแบบดิจิทัล เพื่อให้ได้มาซึ่งหลักฐานทางดิจิทัลเพื่อใช้ในการดำเนินคดีด้านอาชญากรรมไซเบอร์

๙. การแสวงประโยชน์จากช่องโหว่ (Exploitation) หมายถึง การนำเทคนิคการปฏิบัติในมิติไซเบอร์มาดำเนินการกับช่องโหว่หรือใช้ช่องโหว่เป็นทางผ่าน เพื่อให้เกิดผลตามที่ต้องการ

๑๐. ความตระหนักรู้ทางไซเบอร์ (Cyber Awareness, Cyberspace Domain Awareness) หมายถึง ความเข้าใจอย่างถูกต้องเกี่ยวกับสภาวะแวดล้อมและภัยคุกคามในมิติไซเบอร์ในห้วงเวลาหนึ่งหรือตามห้วงเวลาที่ต้องการ มีความเกี่ยวข้องตั้งแต่ระดับบุคคล องค์กร ซึ่งสามารถส่งผลกระทบต่อความมั่นคงของชาติหรือผลประโยชน์แห่งชาติ

๑๑. ความพร้อมในการรับมือทางไซเบอร์ (Cyber Resilience) หมายถึง ความสามารถในการรับมือและฟื้นฟูกลับคืนสู่สภาพปกติโดยเร็วที่สุด หลังจากการถูกโจมตีทางไซเบอร์

๑๒. ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) หมายถึง หลักการ มาตรการ กระบวนการ แนวทางปฏิบัติ เพื่อปกป้องมิติไซเบอร์จากการโจมตีทางไซเบอร์ มักใช้ในบริบทด้านพลเรือน

๑๓. โครงสร้างพื้นฐานวิกฤตของ ทอ. (RTAF Critical Infrastructure) หมายถึง ระบบสาธารณูปโภคที่สำคัญยิ่งสำหรับการปฏิบัติในมิติไซเบอร์ หากถูกโจมตีทางไซเบอร์หรือแสวงประโยชน์จาก ช่องโหว่ จะเกิดผลเสียหายร้ายแรงต่อความสำเร็จของการปฏิบัติภารกิจของ ทอ.เช่น ระบบควบคุมบังคับบัญชา ระบบฐานข้อมูลข่าวกรอง ระบบสนับสนุนการตัดสินใจทางยุทธศาสตร์ ระบบสื่อสารโทรคมนาคม ระบบสื่อสารทางยุทธวิธี ระบบป้องกันทางอากาศ เป็นต้น

๑๔. โครงสร้างพื้นฐานวิกฤตของชาติ (National Critical Infrastructure) หมายถึง ระบบสาธารณูปโภคที่สำคัญยิ่งของรัฐ ซึ่งใช้ระบบสารสนเทศในการควบคุมการปฏิบัติงาน มักใช้ในการให้บริการประชาชน เช่น ระบบการจ่ายกระแสไฟฟ้า ระบบการบริหารจัดการน้ำ ระบบบริการด้านการเงิน ระบบการให้บริการอินเทอร์เน็ต ระบบการสื่อสารทั้งภาคพื้นดินและดาวเทียม ระบบกิจการวิทยุและโทรทัศน์ ระบบการขนส่งมวลชน ระบบควบคุมการจราจรทางบกและทางอากาศ เป็นต้น

๑๕. ช่องโหว่ (Vulnerability) หมายถึง จุดอ่อนหรือข้อบกพร่อง ซึ่งถูกนำมาใช้เพื่อให้ได้ผลตามที่ต้องการ

๑๖. ไซเบอร์ (Cyber) หมายถึง สิ่งที่เกี่ยวข้องหรือสัมพันธ์กับอินเทอร์เน็ต ระบบเครือข่ายคอมพิวเตอร์ ระบบสารสนเทศ ระบบควบคุมกำกับดูแลและเก็บข้อมูล (Supervisory Control and Data Acquisition: SCADA) ระบบควบคุมการทำงานของอุปกรณ์อิเล็กทรอนิกส์ (Embedded Systems) เป็นต้น

๑๗. นักรบไซเบอร์ (Cyber Warrior) หมายถึง บุคคลหรือกลุ่มบุคคลซึ่งปฏิบัติงานในมิติไซเบอร์โดยเน้นการปฏิบัติในลักษณะการโจมตีทางไซเบอร์ หรือแสวงประโยชน์จากช่องโหว่ในมิติไซเบอร์ของฝ่ายตรงข้าม ประกอบด้วยผู้ปฏิบัติงานด้านนโยบาย/ยุทธศาสตร์ รวมทั้งผู้ปฏิบัติงานเชิงเทคนิค

๑๘. โปรแกรมประสงค์ร้าย (Malware) หมายถึง โปรแกรมประสงค์ร้ายต่าง ๆ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูลบนเครื่องคอมพิวเตอร์ของผู้ใช้งาน ตลอดจนโปรแกรมประเภทขโมยข้อมูล และการฝัง Malicious Mobile Code (MMC) ผ่านทางช่องโหว่ของโปรแกรม Internet Browser แบ่งออกได้หลากหลายประเภท เช่น ไวรัส (Virus) เวิร์ม (Worm) โทรจัน (Trojan) การแอบดักจับข้อมูล (Spyware) คีย์ล็อกเกอร์ (Key Logger) ดังนี้

๑๘.๑ ไวรัส (virus) หมายถึง โปรแกรมที่สามารถติดต่อจากอีกไฟล์หนึ่งไปยังอีกไฟล์หนึ่งภายในระบบเดียวกัน หรือจากคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องอื่นโดยการแนบตัวเองไปกับโปรแกรมอื่น สามารถทำลายฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล

๑๘.๒ เวิร์ม (worm) หมายถึง โปรแกรมที่สามารถแพร่กระจายตัวของมันเองได้โดยอัตโนมัติและไม่ต้องอาศัยโปรแกรมอื่นในการแพร่กระจายไปยังคอมพิวเตอร์เครื่องอื่นๆ ผ่านทางเครือข่าย เวิร์ม สามารถทำอันตรายให้กับระบบ

๑๘.๓ โทรจัน (Trojan) หมายถึง โปรแกรมที่ดูเหมือนจะมีประโยชน์หรือไม่เป็นอันตราย แต่ในตัวโปรแกรมจะแฝงโค้ดสำหรับการใช้ประโยชน์หรือทำลายระบบที่ทำงานโดยโปรแกรมนี้ส่วนใหญ่จะถูกแนบมากับจดหมายอิเล็กทรอนิกส์

๑๘.๔ การแอบดักจับข้อมูล (Spyware) หมายถึง โปรแกรมที่ถูกออกแบบมาให้คอยติดตามบันทึกข้อมูลส่วนบุคคล รายงานข้อมูลการใช้งานของผู้ใช้แต่ละคนบนอินเทอร์เน็ต หรือทำการเปลี่ยนการตั้งค่าของโปรแกรมบราวเซอร์ใหม่ ซึ่งก่อให้เกิดความรำคาญ และทำให้ประสิทธิภาพการทำงานของระบบคอมพิวเตอร์ช้าลง

๑๘.๕ คีย์ล็อกเกอร์ (Key Logger) หมายถึง สปายแวร์ประเภทหนึ่งที่ทำหน้าที่บันทึกข้อมูลการกดแป้นคีย์บอร์ดของผู้ใช้ ข้อมูลที่จัดเก็บจะถูกส่งผ่านอินเทอร์เน็ต เพื่อใช้ก่ออาชญากรรมในรูปแบบต่างๆ ได้

๑๙. มิติไซเบอร์ (Cyberspace) หมายถึง มิติที่มีการประยุกต์ใช้หลักการด้านอิเล็กทรอนิกส์และหลักการด้านสเปกตรัมแม่เหล็กไฟฟ้า (Electromagnetic Spectrum) ในการจัดเก็บ แก้ไข หรือแลกเปลี่ยนข้อมูลบนโครงสร้างพื้นฐานทางกายภาพ

๑๙.๑ อิเล็กทรอนิกส์ (Electronics) หมายถึง หลักการที่เกี่ยวข้องกับการออกแบบวงจรไฟฟ้า (Circuits) โดยใช้ทรานซิสเตอร์ (Transistors) และไมโครชิป (Microchips) รวมไปถึงหลักการที่เกี่ยวข้องกับพฤติกรรมและการเคลื่อนที่ของอิเล็กตรอนในสารกึ่งตัวนำ (Semiconductor) ตัวนำ (Conductor) สุญญากาศ หรือก๊าซ

๑๙.๒ สเปกตรัมแม่เหล็กไฟฟ้า (Electromagnetic Spectrum) หมายถึง หลักการที่เกี่ยวข้องกับช่วงหรือแถบคลื่นแม่เหล็กไฟฟ้าซึ่งมีความยาวที่แตกต่างกัน ใช้ในด้านการสื่อสารโทรคมนาคมแบบต่าง ๆ ตามคุณสมบัติของแต่ละช่วงคลื่น

๑๙.๓ การปฏิบัติในมิติไซเบอร์ (Cyberspace Operations) หมายถึง การดำเนินการโดยใช้ขีดความสามารถทางไซเบอร์ในมิติไซเบอร์ เพื่อให้บรรลุวัตถุประสงค์ที่ตั้งไว้

๒๐. ยุทธภัณฑ์ทางไซเบอร์ (Cyber Weapon) หมายถึง ระบบชุดของยุทโธปกรณ์ หรือชุดคำสั่งทางคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ซึ่งใช้ในการโจมตีทางไซเบอร์หรือแสวงประโยชน์จากช่องโหว่ในมิติไซเบอร์ของฝ่ายตรงข้าม

๒๑. สงครามไซเบอร์ (Cyber warfare) หมายถึง การปฏิบัติในมิติไซเบอร์ซึ่งมีมูลเหตุหรือวัตถุประสงค์ทางการเมืองหรือทางทหาร โดยนำเทคนิคการปฏิบัติในมิติไซเบอร์มาใช้ป้องกัน รวมทั้งโจมตีหรือแสวงประโยชน์จากช่องโหว่ในมิติไซเบอร์ของฝ่ายตรงข้าม

๒๒. เหตุคุกคามทางไซเบอร์ (Cyber Incident) หมายถึง เหตุการณ์ (Event) ที่ไม่เป็นไปตามนโยบายหรือมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งอาจบ่งบอกถึงการถูกโจมตีทางไซเบอร์หรือการถูกแสวงประโยชน์จากช่องโหว่ ได้แก่ ความพยายามเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต (Unauthorized Access) เหตุการณ์ขัดขวางหรือทำให้ระบบสารสนเทศไม่สามารถใช้งานได้ (Disruption or Denial of Service) หรือเหตุการณ์พยายามเปลี่ยนแปลงข้อกำหนดทางเทคนิคของระบบสารสนเทศ เป็นต้น

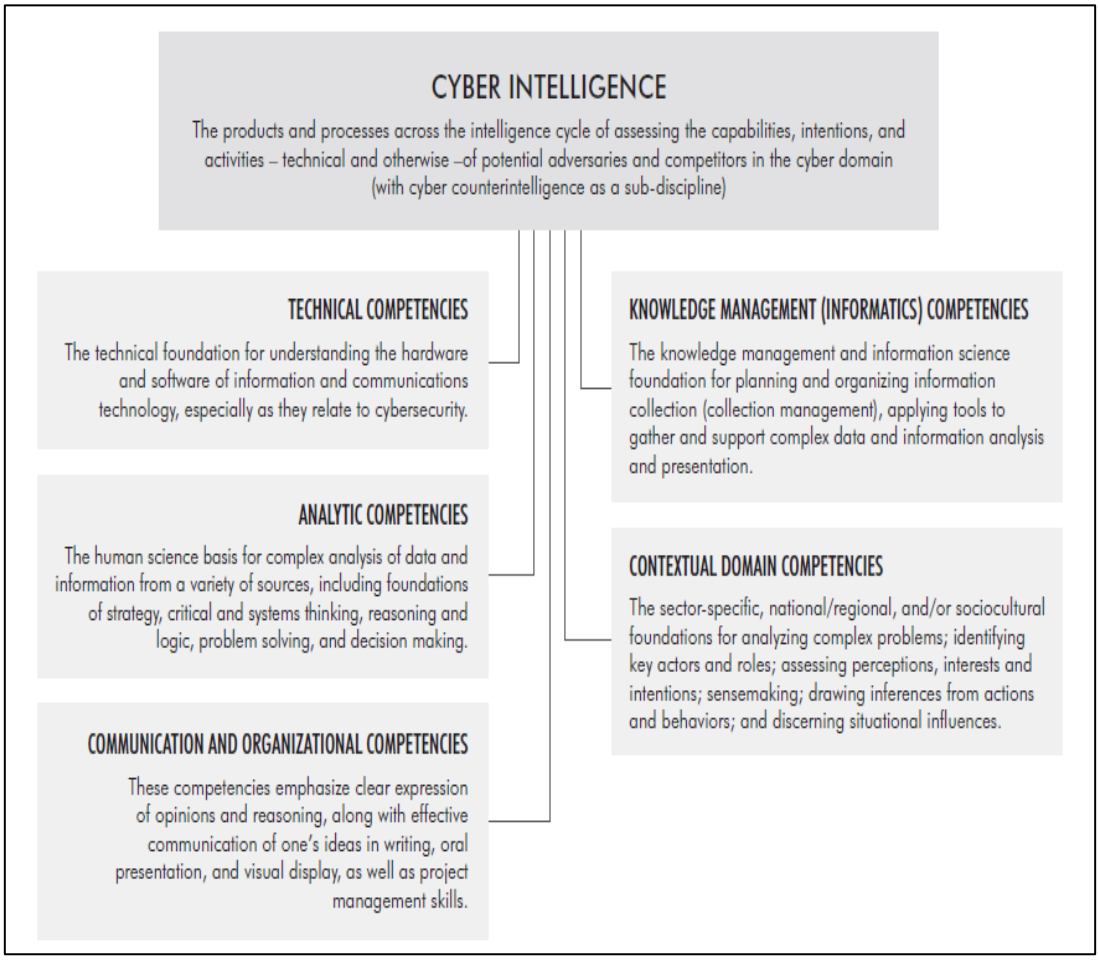
ผนวก ข ผลงานวิจัยที่เกี่ยวข้อง

Jay McAllister ได้ทำการศึกษาเรื่องการประยุกต์กระบวนการคิดเชิงวิพากษ์ เพื่อนำมาใช้กับงานข่าวกรองไซเบอร์ สรุปว่านักวิเคราะห์ในทุกระดับควรอุทิศเวลาให้กับการพัฒนาวิธีการคิด โดยการลงลึกไปถึงกระบวนการทำงานของจิตใจมนุษย์ เพื่อปรับปรุงทักษะการวิเคราะห์ ซึ่งผู้วิจัยพบว่าหลักวิธีเช่นนี้ไม่ต่างกับการวิเคราะห์ข่าวกรองชนิดอื่นๆ

Robert M. Lee ทำการศึกษางานข่าวกรองไซเบอร์เพื่อบรรยายในหลักสูตรบัณฑิตศึกษาด้านความมั่นคงและปลอดภัยทางไซเบอร์ สรุปว่าขั้นตอนแรกในการเข้าใจงานข่าวกรองไซเบอร์ คือการเข้าใจวงรอบข่าวกรองทั้งในด้านยุทธวิธี เทคนิค และขั้นตอนการปฏิบัติ ซึ่งการดาเนินการข่าวกรอง ประเภทต่าง ๆ มีอยู่นานก่อนที่จะเกิดงานข่าวกรองไซเบอร์ โดยเฉพาะด้านการตัดสินตกลงใจทางทหารที่ ผู้บังคับบัญชา ต้องการทราบเจตนารมณ์ของฝ่ายตรงข้ามเพื่อเลือกยุทธศาสตร์ที่ดีกว่าในสนามรบหรือ เตรียมตัวให้พร้อมสาหรับการโจมตี รวมถึงการป้องกันอย่างเหมาะสม เพราะฉะนั้นการเริ่มศึกษาข่าวกรอง ไซเบอร์สามารถเริ่มได้จากการศึกษาแนวทางข่าวกรองทหาร

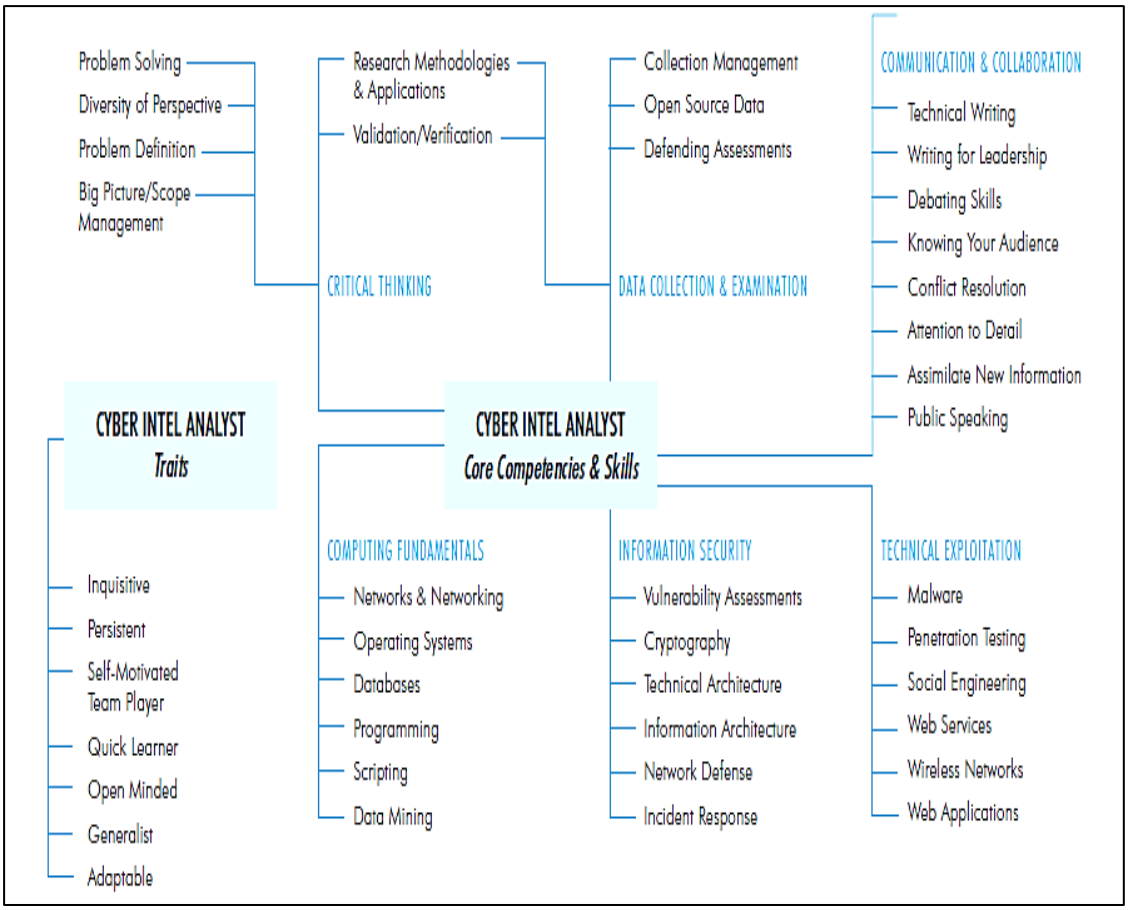
เครือข่าย Intelligence and National Security Alliance ระบุว่า ข่าวกรองไซเบอร์ คือการประเมินขีดความสามารถ เจตนารมณ์ และกิจกรรมของข้าศึก ในห้วงมิติทางไซเบอร์ (Cyber Domain) เพื่อสนับสนุนการแจ้งเตือน การโจมตี และการป้องกันภัยคุกคาม ซึ่งเป็นผลผลิตที่ได้จากการดำเนิน วงรอบข่าวกรองโดยมีขีดความสามารถที่จำเป็น ได้แก่

๑. ความเข้าใจในเรื่องของระบบฮาร์ดแวร์ ซอฟต์แวร์ ระบบสารสนเทศและการสื่อสาร
๒. ทักษะการคิดวิเคราะห์
๓. การนำเสนอ รายงาน ให้ความเห็นที่เป็นเหตุเป็นผล
๔. การบริหารจัดการวางแผนรวบรวมข้อมูลข่าวกรอง
๕. ความเข้าใจในภารกิจ และบริบทของหน่วยงาน เช่น ผู้แสดงหลัก กลุ่มผลประโยชน์



ภาพที่ ข-๑ ขีดความสามารถที่จำเป็นของงานข่าวกรองไซเบอร์[๑๒]

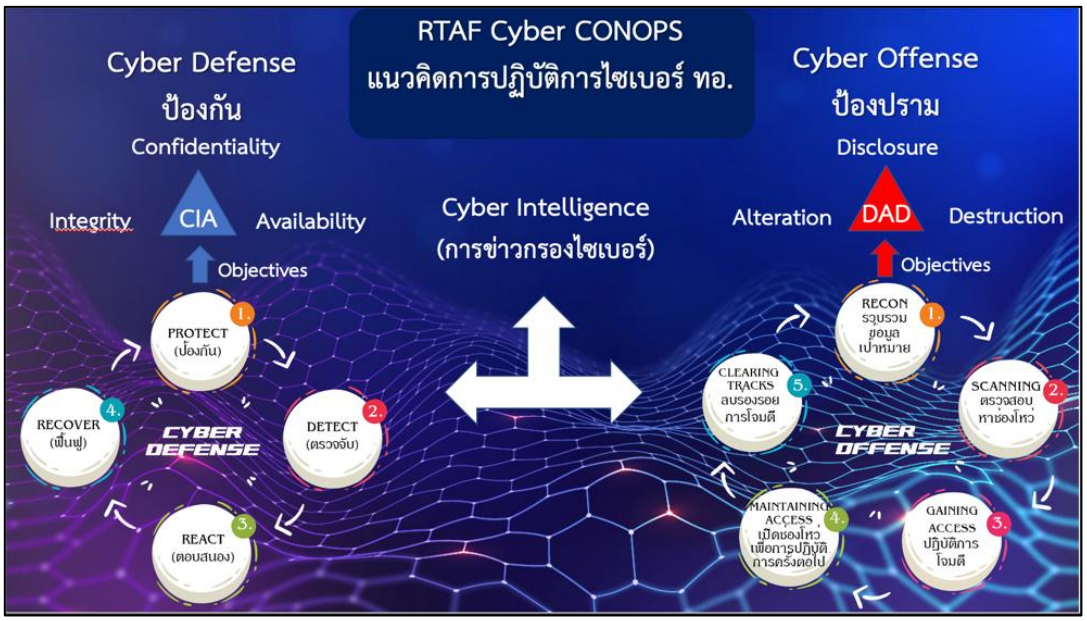
[๑๒] CTI –EU | Bonding EU Cyber Threat Intelligence ENISA, Online, 2017



ภาพที่ ข-๒ ขีดความสามารถและทักษะที่จำเป็นของนักวิเคราะห์ข่าวกรองทางไซเบอร์[๑๓]

[๑๓] Information Security Education Carnegie Mellon University, Online, 2017

ผนวก ค หลักนิยมการปฏิบัติการไซเบอร์ในกองทัพอากาศ



ภาพที่ ค-๑ แนวคิดการปฏิบัติการไซเบอร์ ทอ.[14]

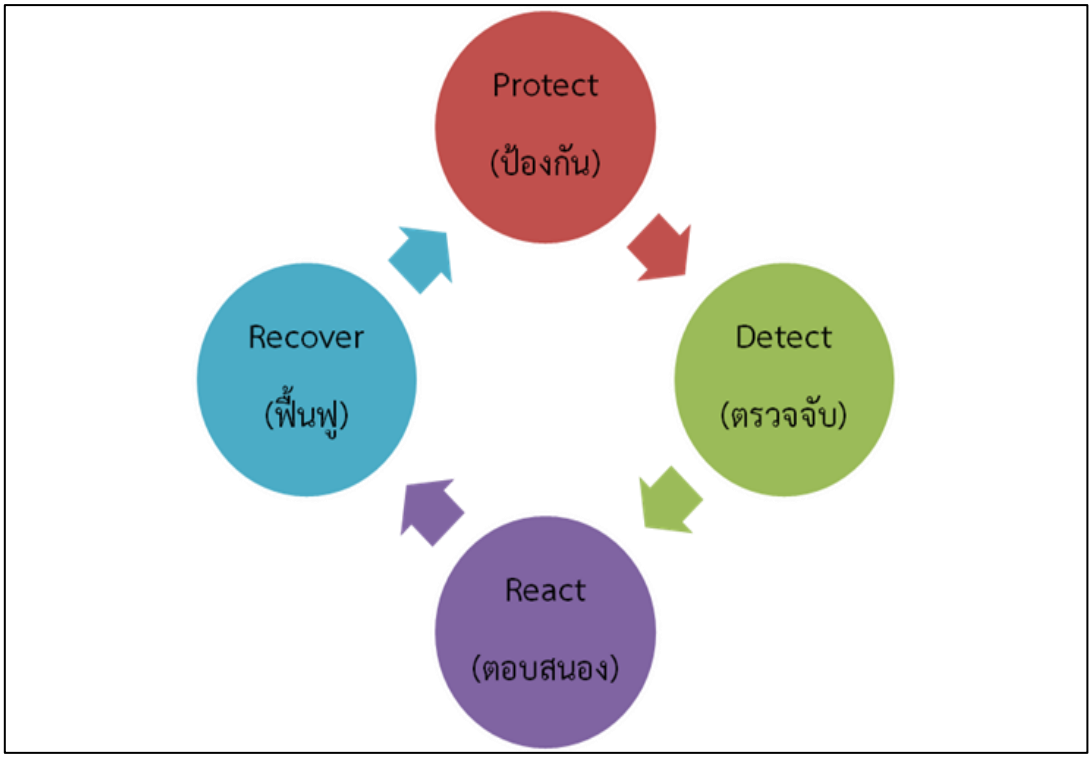
แนวคิดการปฏิบัติการไซเบอร์ ทอ.

๑. ปฏิบัติการไซเบอร์เชิงรับ เป็นการเฝ้าระวังป้องกันและตรวจจับการบุกรุก สืบค้นจุดอ่อนและช่องโหว่ในระบบไซเบอร์ของฝ่ายเรา รวมทั้งการสำรองและกู้คืนระบบกรณีถูกโจมตีทางไซเบอร์จากฝ่ายตรงข้าม

๒. ปฏิบัติการไซเบอร์เชิงรุก เป็นการดักรับข้อมูลการใช้งานทางไซเบอร์ การก่อกวนระบบคอมพิวเตอร์ จำกัดเสรีภาพในการใช้งาน และทำให้เครื่องคอมพิวเตอร์แม่ข่ายปฏิเสธการให้บริการหรือหยุดการทำงาน รวมถึงสามารถจารกรรมข้อมูลของฝ่ายตรงข้ามได้ในระดับหนึ่ง โดยระวังป้องกันและรักษาความปลอดภัยระบบสารสนเทศของหน่วยและระบบ ให้ปฏิบัติตามระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของ ทอ. พ.ศ.๒๕๕๒ หรือฉบับที่มีผลบังคับใช้อย่างเคร่งครัด

๓. ปฏิบัติการข่าวกรองไซเบอร์ มีเป้าหมายเพื่อ วางแผน รวบรวม วิเคราะห์ ข่าวกรองเพื่อสนับสนุนการปฏิบัติการทั้งเชิงรุกและเชิงรับเพื่อให้ประสบความสำเร็จในการปฏิบัติการเชิงรับ มีการปฏิบัติดังนี้

[14] RTAF Cyber CONOPS



ภาพที่ ค-๒ วงรอบการปฏิบัติ Cyber Defense

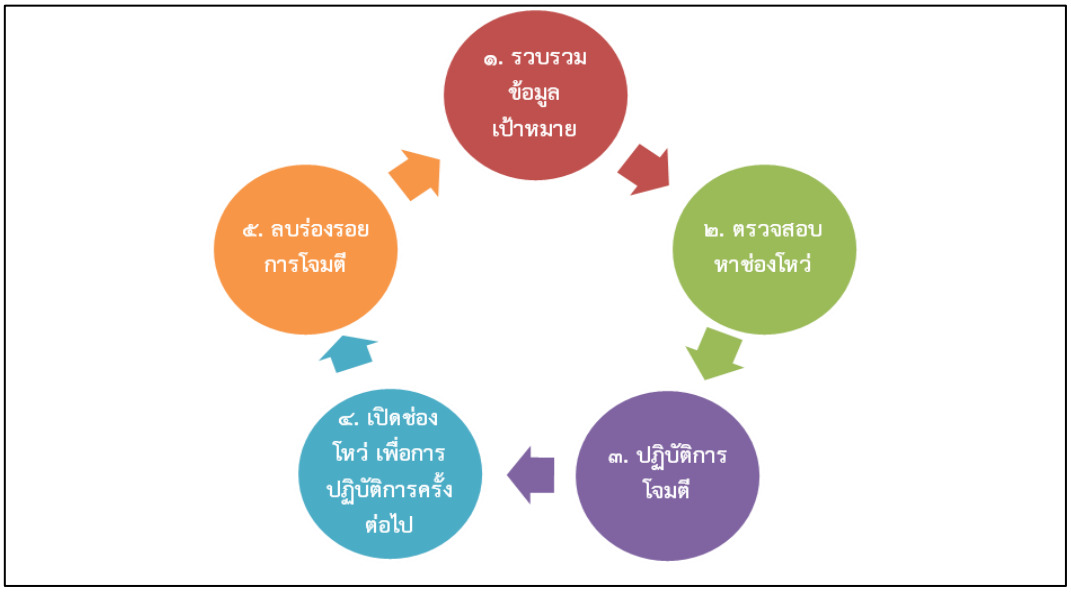
๓.๑ การป้องกัน เน้นย้ำให้ นกข.ต้องระวังป้องกันระบบไซเบอร์ที่ตนเองรับผิดชอบตามแนวทางของระเบียบฯ และนโยบายด้านความมั่นคงฯ ที่เกี่ยวข้อง โดยมีทีมชุดปฏิบัติการด้านสงครามไซเบอร์ เป็นผู้รับผิดชอบในการประเมินมาตรการรักษาความมั่นคงปลอดภัย

๓.๒ การตรวจจับ เน้นย้ำให้ นกข.ผู้รับผิดชอบการระวังป้องกัน ต้องเฝ้าระวัง และรายงานเหตุการณ์ล่วงละเมิดความมั่นคงปลอดภัยด้านไซเบอร์ให้ทันเวลา เพื่อให้สามารถตอบสนองและแก้ไขได้ทันท่วงที

๓.๓ การตอบสนอง เน้นย้ำให้ นกข.ต้องปฏิบัติการแก้ปัญหาการล่วงละเมิด การรักษาความมั่นคงปลอดภัย ไซเบอร์ โดยทันทีตามมาตรการที่เหมาะสม เพื่อป้องกันระบบสารสนเทศไม่ให้ส่งผลกระทบกับระบบบัญชาการและควบคุม รวมทั้งระบบอื่นที่เกี่ยวข้อง ตลอดจนระงับเหตุล่วงละเมิดการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๔ การฟื้นฟู เน้นย้ำให้ นกข.ต้องปฏิบัติการฟื้นฟูระบบที่ได้รับผลกระทบทั้งหมด เพื่อให้กลับคืนสู่สภาพปกติพร้อมใช้งานโดยเร็วที่สุด และปรับปรุงกระบวนการป้องกันให้ดียิ่งขึ้น

๔. การปฏิบัติการไซเบอร์เชิงป้องปราม/ตอบโต้ มีการปฏิบัติดังนี้



ภาพที่ ค-๓ วงรอบการปฏิบัติ Cyber Attack

๔.๑ การรวบรวมข้อมูลเป้าหมาย ต้องปฏิบัติอย่างจริงจังในกระบวนการรวบรวมข้อมูลเกี่ยวกับเป้าหมายในทุกด้าน เพื่อใช้ในการวิเคราะห์หาช่องโหว่

๔.๒ การตรวจสอบหาช่องโหว่ ต้องปฏิบัติอย่างจริงจังในการวิเคราะห์หาช่องโหว่โดยใช้ข้อมูลจากการรวบรวมเป้าหมาย เพื่อเตรียมการโจมตีตามช่องโหว่ที่ค้นพบ

๔.๓ การปฏิบัติการโจมตี ต้องวางแผนและดำเนินการโจมตี เพื่อให้บรรลุเป้าหมายตามคำสั่งที่ได้รับ โดยขั้นตอนนี้ต้องดำเนินการแบบพราง เพื่อไม่ให้สืบย้อนมาถึงเราได้

๔.๔ การเปิดช่องโหว่ เพื่อการปฏิบัติการครั้งต่อไป ให้ปฏิบัติโดยการฝังทางลับ (Backdoor) เพื่อการเข้าปฏิบัติการในครั้งต่อไป

๔.๕ การลบร่องรอยการโจมตี ให้ปฏิบัติโดยการ กลบเกลื่อน ร่องรอย เพื่อไม่ให้สืบย้อนมาถึงหน่วยงาน ทอ.ได้

ผนวก ง การนำผลงานวิจัยไปใช้ประโยชน์

งานวิจัยนี้มีจุดมุ่งหมายที่สำคัญในการศึกษาและทดสอบ Cyber Threat Intelligence Feeds หลายแหล่ง เพื่อปรับใช้กับระบบข่าวกรองภัยคุกคามทางไซเบอร์แบบไม่เสียค่าใช้จ่าย เพื่อเป็นการพัฒนายกระดับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศ บนพื้นฐานของการพัฒนาอย่างยั่งยืน ผ่านการลดการพึ่งพาเทคโนโลยีผ่านการจัดซื้อจัดหา โดยผลงานวิจัยนี้เกิดประโยชน์ต่อกองทัพอากาศทั้งในระยะสั้นและระยะยาว โดยมีรายละเอียดดังนี้

สภาพการณ์ก่อนการวิจัยและพัฒนา

ก่อนการวิจัยและพัฒนา หน่วยงานภายในกองทัพอากาศยังไม่มีระบบวิเคราะห์ภัยคุกคามทางไซเบอร์ที่สามารถบูรณาการข้อมูลจากหลายแหล่งแบบอัตโนมัติ การตรวจสอบภัยคุกคามอาศัยการประเมินแบบแยกส่วนจากแหล่งข้อมูลที่แตกต่างกัน ทำให้เกิดช่องว่างในการเฝ้าระวังและตอบโต้ภัยคุกคามได้อย่างมีประสิทธิภาพ สำหรับการเปรียบเทียบก่อน-หลัง การวิจัยและพัฒนามีรายละเอียดตามตารางดังนี้

เกณฑ์เปรียบเทียบ	ก่อนใช้แพลตฟอร์ม (๒๕๖๖)	หลังใช้แพลตฟอร์ม (๒๕๖๗)	เครื่องมือเชิงพาณิชย์
การตรวจจับภัยคุกคาม	พึ่งพาการรายงานแบบแมนนวล และมีข้อจำกัดในการวิเคราะห์ข้อมูลจากหลายแหล่ง	มีการตรวจจับอัตโนมัติเชื่อมโยงกับ OpenCTI และแจ้งเตือนแบบเรียลไทม์	สามารถวิเคราะห์ภัยคุกคามขั้นสูงและเชื่อมต่อกับ Threat Intelligence ระดับสากล
การตอบสนองต่อภัยคุกคาม	ใช้เวลาตอบสนองเฉลี่ย ๓ - ๕ วัน	ลดเวลาตอบสนองลงเหลือ ๑ - ๒ วัน	มีความสามารถในการตอบสนองอัตโนมัติ
การระบุภัยคุกคามที่แท้จริง	ข้อมูลภัยคุกคามมีการกรองได้น้อย ทำให้เกิด False Positive สูง	สามารถเชื่อมต่อกับฐานข้อมูลภัยคุกคาม ทำให้ความแม่นยำเพิ่มขึ้น	มีความแม่นยำสูงในการตรวจจับภัยคุกคาม
การบันทึกและติดตาม	ไม่มีแพลตฟอร์มกลางสำหรับรวบรวมข้อมูล	สามารถบันทึกและติดตามข้อมูลภัยคุกคามได้อย่างเป็นระบบ	มีแดชบอร์ดที่แสดงข้อมูลแบบละเอียดและสามารถบูรณาการกับ SIEM ได้

ดังนั้น การพัฒนาที่เกิดขึ้นจากงานวิจัยนี้ ผู้วิจัยได้พัฒนาต้นแบบระบบ Cyber Threat Intelligence Feeds ที่สามารถรวบรวม วิเคราะห์ และแจ้งเตือนภัยคุกคามไซเบอร์จากหลายแหล่งข้อมูลได้แบบเรียลไทม์ นอกจากนี้ยังสามารถบูรณาการกับระบบข่าวกรองไซเบอร์ของกองทัพอากาศ เพื่อเพิ่มความสามารถในการรับมือภัยคุกคามไซเบอร์ได้อย่างแม่นยำและรวดเร็วขึ้น โดยมีศักยภาพในการปฏิบัติการที่เทียบเคียงกับเครื่องมือเชิงพาณิชย์

แนวทางการนำไปใช้ประโยชน์

งานวิจัยนี้ สามารถเป็นแนวทางเพื่อนำไปใช้ประโยชน์ในกองทัพอากาศได้อย่างเป็นรูปธรรม โดยผลกระทบ (Impact) ที่เกิดขึ้นจากงานวิจัยนี้ ส่งผลในการพัฒนาด้านการข่าวกรองไซเบอร์ ทั้งในแง่การเตรียมบุคลากรให้พร้อม การปรับปรุงแนวทางการปฏิบัติเพื่อรองรับการนำระบบที่ได้จากการวิจัยไปใช้ประโยชน์ โดยมีรายละเอียดดังนี้

๑. การเพิ่มเนื้อหาในการทดสอบความตระหนักรู้ทางไซเบอร์ของกองทัพอากาศ

การพัฒนาเครื่องมือที่ช่วยเสริมสร้างความตระหนักรู้ทางไซเบอร์ให้กับกำลังพล โดยการจัดทำกรณีศึกษาและการทดสอบจำลองสถานการณ์ภัยคุกคามเพื่อให้บุคลากรมีความพร้อมรับมือกับเหตุการณ์ทางไซเบอร์ได้ดียิ่งขึ้น โดยมีการพัฒนาปรับปรุงเนื้อหาการทดสอบความตระหนักรู้ทางไซเบอร์ของกองทัพอากาศ ให้มีความทันสมัยและรองรับองค์ความรู้ที่ได้จากงานวิจัยดังกล่าว

๒. การสนับสนุนการขับเคลื่อนนโยบายผู้บัญชาการทหารอากาศ

งานวิจัยนี้ช่วยส่งเสริมการพัฒนาขีดความสามารถของกำลังพลในการปฏิบัติการข่าวกรองทางไซเบอร์ และเสริมสร้างความสามารถเชิงรุกในการป้องกันและรับมือภัยคุกคามในหลายมิติ รวมถึงการพัฒนาระบบ Cyber Threat Intelligence (CTI) และการฝึกซ้อมสถานการณ์การป้องกันโครงสร้างพื้นฐานสำคัญของกองทัพอากาศจากการโจมตีทางไซเบอร์ ตามนโยบายของผู้บัญชาการทหารอากาศ ผ่านแผนงานและโครงการที่ถูกจัดทำขึ้น

๓. การสำรวจข้อมูลการดำเนินการทางไซเบอร์จากหน่วยงานภายในกองทัพอากาศ

งานวิจัยนี้ส่งผลให้มีการปรับปรุงแนวทางการจัดทำฐานข้อมูลเกี่ยวกับการดำเนินการทางไซเบอร์ของหน่วยงานภายในกองทัพอากาศเพื่อให้สามารถใช้เป็นแนวทางในการพัฒนาและปรับปรุงมาตรการความปลอดภัยทางไซเบอร์ให้มีประสิทธิภาพมากขึ้น

๔. การจัดทำข้อกำหนดเพิ่มเติมงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

งานวิจัยนี้ส่งผลต่อการพัฒนากฎระเบียบและมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ให้ครอบคลุมทุกภาคส่วนของกองทัพอากาศ รวมถึงกำหนดมาตรฐานสำหรับการเฝ้าระวังและการจัดการภัยคุกคามทางไซเบอร์

๕. การปรับรูปแบบการรายงานใช้กำลังมิติไซเบอร์

งานวิจัยนี้ส่งผลให้เกิดการปรับปรุงกระบวนการรายงานและการวิเคราะห์ข้อมูลด้านภัยคุกคามไซเบอร์ให้มีประสิทธิภาพมากขึ้น โดยการนำระบบอัตโนมัติเข้ามาช่วยเสริมความสามารถในการติดตาม วิเคราะห์ และจัดทำรายงานเกี่ยวกับภัยคุกคามทางไซเบอร์ของกองทัพอากาศ

หน่วยงานที่ใช้ประโยชน์จริงและข้อเสนอแนะจากผู้ใช้

แพลตฟอร์มดังกล่าวถูกนำไปใช้งานโดยหน่วยงานที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ของกองทัพอากาศรวมถึงหน่วยงานนอกกองทัพอากาศ เช่น สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หน่วยงานในกระทรวงกลาโหมเช่น ศูนย์ไซเบอร์ทหาร ศูนย์ไซเบอร์ของแต่ละเหล่าทัพ นอกจากนี้ ยังเป็นจุดเริ่มต้นของการสร้างความร่วมมือด้านข่าวกรองทางไซเบอร์ของหน่วยงานในประชาคมไซเบอร์ต่างประเทศ เช่น Cyber Defence Working Group และ Cyber SMEE

เมื่อพิจารณารายละเอียดหน่วยงานของกองทัพอากาศ ในการประยุกต์ใช้งานวิจัยนี้พบว่า

๑. ศูนย์ไซเบอร์กองทัพอากาศ เป็นหน่วยงานหลักที่ใช้แพลตฟอร์มนี้ในการตรวจจับและวิเคราะห์ภัยคุกคาม ใช้แพลตฟอร์มในการสนับสนุนการตัดสินใจและการวางแผนรับมือภัยคุกคาม

๒. กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ สามารถใช้ผลการวิจัยและข้อมูลจากระบบนี้ในการกำหนดนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงการประสานงานและแจ้งเตือนเหตุการณ์ไซเบอร์ได้อย่างมีประสิทธิภาพมากขึ้น รวมถึงกำหนดแนวทางการพัฒนาศักยภาพด้านไซเบอร์ของกองทัพอากาศในภาพรวมที่อยู่บนพื้นฐานการพึ่งพาตนเองได้

๓. กรมยุทธการทหารอากาศสามารถนำไปใช้ประโยชน์ในงานด้านการฝึกการใช้กำลังทางไซเบอร์ และการใช้กำลังผ่านการปฏิบัติการข้อมูลข่าวสาร (Information Operations: IO)

๔. กรมข่าวทหารอากาศ สามารถใช้ข้อมูลที่ได้รับจากระบบที่พัฒนาจากงานวิจัยนี้เพื่อรับมอบหัวข้อข่าวสารสำคัญ เช่น แผนลาดตระเวน และข่าวกรองทางไซเบอร์ เป็นต้น

๕. หน่วยขึ้นตรงกองทัพอากาศ สามารถใช้ประโยชน์จากงานวิจัยดังกล่าว ในการส่งเสริมให้กำลังพลของหน่วยมีความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงการรับรู้ข้อมูลข่าวกรองทางไซเบอร์ที่เกี่ยวข้องในการสร้างการป้องกันภัยทางไซเบอร์เชิงรับได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะจากผู้ใช้

เมื่อนำงานวิจัยนี้ไปทดสอบใช้งานตามหน่วยงานต่าง ๆ ของกองทัพอากาศ ผู้วิจัยได้ทำการประเมินผล และได้รับข้อเสนอแนะจากผู้ใช้งานดังนี้

๑. ปรับปรุง UI/UX ให้ใช้งานง่ายขึ้น – บางหน่วยงานพบว่าอินเทอร์เฟซยังต้องการการปรับปรุงให้เข้าถึงข้อมูลได้เร็วขึ้น

๒. เพิ่มความสามารถในการตรวจจับภัยคุกคามแบบ Zero-Day – ปัจจุบันแพลตฟอร์มอาจยังขาดความสามารถในการตรวจจับภัยคุกคามที่ไม่เคยปรากฏมาก่อน

๓. รองรับการบูรณาการกับ SIEM และระบบ Log Analysis อื่น ๆ – เพื่อให้สามารถเชื่อมต่อข้อมูลกับระบบที่มีอยู่แล้วได้ง่ายขึ้น

๔. พัฒนาความสามารถด้าน Machine Learning – เพื่อให้ระบบสามารถเรียนรู้และพัฒนาอัลกอริธึมในการวิเคราะห์ภัยคุกคามได้แม่นยำขึ้น