

การจัดการเรียนรู้โดยใช้แพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF) Cybersecurity Education Based on Capture the Flag (CTF) Platforms

บทความวิชาการ

สิริวรรณ อินทสร

Siriwan Intasorn

กองวิชาคณิตศาสตร์ ส่วนการศึกษา โรงเรียนเตรียมทหาร สถาบันวิชาการป้องกันประเทศ นครนายก ประเทศไทย 26110

Mathematic Division, Armed Forces Academies Preparatory School,

National Defense Studies Institute, Nakhon Nayok, Thailand, 26110

E-mail: siriwan.int@ndsi.ac.th

บทคัดย่อ

บทความนี้มีวัตถุประสงค์เพื่อนำเสนอการศึกษาการนำแพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF) ซึ่งเป็นเกมการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์ ที่มีการนำมาใช้เป็นสื่อการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ โดยที่ผู้เรียนจะพัฒนาทักษะการใช้เครื่องมือด้านการรักษาความมั่นคงทางไซเบอร์จากการแข่งขันเกมยึดธง (CTF) ซึ่งมีหมวดหมู่ทักษะการรักษาความปลอดภัยทางไซเบอร์ 2 ด้าน ประกอบด้วย ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เชิงรุกและด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เชิงรับ ซึ่งมีหมวดหมู่ที่นิยมใช้บนแพลตฟอร์มเกมยึดธงทางไซเบอร์สำหรับฝึกฝนและในการแข่งขัน 10 หมวดหมู่ ได้แก่ การเขียนโปรแกรม (Programming) การเข้าถึงทรัพยากรของเครือข่าย (Network Exploitations) การเข้าถึงทรัพยากรของเว็บ (Web Exploitations) การยึดครองควบคุมเครื่อง (Pwnable/Binary Exploitations) การทำวิศวกรรมย้อนกลับ (Reverse Engineering) การตรวจพิสูจน์ทางดิจิทัล (Digital Forensics) วิทยาการเข้ารหัสลับ (Cryptography) การใช้เครื่องมือข่าวกรองทางแหล่งข้อมูลเปิด (Open-Source Intelligence: OSINT) ความรู้เบ็ดเตล็ด (Miscellaneous) การรักษาความปลอดภัยบนอุปกรณ์เคลื่อนที่ (Mobile Security) ทั้งนี้ รูปแบบการเรียนรู้ผ่านแพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF) เป็นการจำลองยุทธทางไซเบอร์ที่มีประโยชน์ต่อการให้ผู้เรียนได้ทำงานผ่านความท้าทายหลายอย่างโดยใช้เทคโนโลยีทางไซเบอร์และเลือกใช้ AI ได้อย่างสร้างสรรค์และมีจริยธรรม

คำสำคัญ : การรักษาความมั่นคงปลอดภัยทางไซเบอร์, เกมยึดธง, แพลตฟอร์มเกมยึดธงทางไซเบอร์

Abstract

This article aims to present a study on cybersecurity education based on Capture The Flag (CTF) platforms. The students will develop cybersecurity skills by using cyber security tools in Capture the Flag Competitions. Types of CTF challenges are divided into 2 areas of cybersecurity knowledge, offensive security skills and defensive security skills and consist of 10 categories commonly used for training and competition as follows: 1) Programming 2) Network Exploitation 3) Web Exploitation 4) Pwnable Binary Exploitation 5) Reverse Engineering 6) Digital Forensics 7) Cryptography 8) OSINT: Open-Source Intelligence 9) Miscellaneous 10) Mobile Security. Cybersecurity education based on Capture the Flag (CTF) Platforms is a useful learning approach that simulates cybersecurity scenarios and allows students to work through various challenges while using cybersecurity technologies and AI tools in creative and ethical ways.

Keywords: Cybersecurity Education, Capture the Flag Competitions, Capture the Flag Platforms

บทนำ

ในปัจจุบันเทคโนโลยีดิจิทัลได้มีบทบาทในชีวิตของพลเมืองไทยและในหน่วยงานทั้งภาครัฐ และภาคเอกชน

และเพื่อให้ประเทศไทยสามารถสร้างสรรค์และใช้เทคโนโลยีดิจิทัลได้อย่างเต็มศักยภาพ การพัฒนาโครงสร้างพื้นฐาน นวัตกรรม ข้อมูล ทุนมนุษย์ และทรัพยากรอื่นใด เพื่อขับเคลื่อนการพัฒนาเศรษฐกิจและสังคมของประเทศไปสู่ความมั่นคง มั่งคั่ง และยั่งยืนจึงเป็นสิ่งสำคัญ จากแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช., 2562) ได้ให้ความสำคัญกับการใช้นวัตกรรมและเทคโนโลยีดิจิทัล การสร้างโอกาสทางสังคมด้วยข้อมูลข่าวสารและบริการต่าง ๆ ผ่านสื่อดิจิทัล อีกทั้งเตรียมความพร้อมให้บุคลากรทุกกลุ่มให้มีความรู้และทักษะที่เหมาะสมต่อการดำเนินชีวิตและการประกอบอาชีพในยุคดิจิทัล รวมทั้งปฏิรูปกระบวนการต้นการทำงานและการให้บริการของภาครัฐ ด้วยเทคโนโลยีดิจิทัลและการใช้ประโยชน์จากข้อมูล สอดคล้องควบคู่กับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช., 2565) ได้นำเสนอนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570) ซึ่งปัจจุบันเทคโนโลยีดิจิทัลมีบทบาทสำคัญในการเป็นเครื่องมืออำนวยความสะดวกแก่การดำรงชีวิตประจำวัน โดยรายงานของ International Telecommunication Union (ITU, 2018) พบว่า ปี พ.ศ. 2561 มีจำนวนผู้ใช้อินเทอร์เน็ต คิดเป็นร้อยละ 51 ของประชากรทั่วโลก โดยคาดว่า ภายในปี พ.ศ. 2566 จะมีจำนวนผู้ใช้งานอินเทอร์เน็ตเพิ่มขึ้นถึงร้อยละ 70 ของประชากรทั่วโลก ทั้งนี้ผลสำรวจพฤติกรรมผู้ใช้งานอินเทอร์เน็ตในประเทศไทย ปีพ.ศ. 2561 โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ., 2562) พบว่า ประเทศไทยก้าวสู่สังคมดิจิทัลอย่างเต็มรูปแบบแล้ว ซึ่งค่าเฉลี่ยของการใช้งานอินเทอร์เน็ตของคนไทยเติบโตเพิ่มขึ้นมากกว่าปีที่ผ่านมาถึง 3 เท่า ทั้งนี้ความก้าวหน้าทางเทคโนโลยีดิจิทัล โดยเฉพาะอย่างยิ่งการใช้อินเทอร์เน็ตมาพร้อมกับความท้าทาย และภัยคุกคาม

ทางไซเบอร์มีหลากหลายรูปแบบ ไม่ว่าจะเป็นการเผยแพร่ข้อมูลที่ไม่เป็นจริง การพยายามบุกรุกเข้าสู่ระบบ การโจมตีสภาพการใช้งานของระบบ การพัฒนาโปรแกรมที่ไม่พึงประสงค์ และการสร้างเว็บไซต์ปลอมเพื่อหลอกลวงหาผลประโยชน์ เป็นต้น อันก่อให้เกิดความเสียหายแก่ประเทศชาติ ภาครัฐกิจ และปัจเจกบุคคล จึงได้มีนโยบายสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ ทั้งด้านบุคลากร องค์ความรู้ และเทคโนโลยี เพื่อเสริมสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยบูรณาการ บุคลากร องค์ความรู้ และเทคโนโลยี นำไปสู่การพัฒนาผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมของประเทศ จึงได้มีการส่งเสริมให้พัฒนาหลักสูตรการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ทั้งภาคทฤษฎีและภาคปฏิบัติเป็นสาขาเฉพาะทางในระดับอุดมศึกษา เพื่อรองรับความต้องการของภาคอุตสาหกรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ รวมทั้งพัฒนาทักษะและฝึกอบรมบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในระดับผู้บริหารและปฏิบัติงาน

การศึกษาเรื่องความปลอดภัยทางไซเบอร์จึงมีความสำคัญมากจากความต้องการผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์เพิ่มขึ้น ทักษะการปฏิบัติการทางไซเบอร์เป็นองค์ประกอบสำคัญของการศึกษาด้านความปลอดภัยทางไซเบอร์และหมวดหมู่ทักษะการรักษาความปลอดภัยทางไซเบอร์มีหลากหลายด้าน จึงได้มีการใช้นวัตกรรมทางการศึกษาในรูปแบบของแพลตฟอร์มเกมการยึดธงทางไซเบอร์ (CTF) มาใช้อย่างแพร่หลายและเป็นที่นิยมเพิ่มมากขึ้นเรื่อย ๆ และกลายเป็นเครื่องมือสำคัญในการพัฒนาการศึกษา จากจัดการแข่งขัน (Capture the Flag Thailand [CTF Thailand], 2566b) ที่มีการร่วมมือกันระหว่างองค์การภาครัฐและเอกชนในการจัดกิจกรรมการแข่งขันแบบออนไลน์และออนไลน์เพื่อดึงดูดให้นักเรียน

นักศึกษาและบุคคลทั่วไปได้ฝึกฝนและทดสอบทักษะการรักษาความปลอดภัยทางไซเบอร์นอกจากนี้ มีงานวิจัยที่นำแพลตฟอร์มเกมการยึดธงทางไซเบอร์ (CTF) มาใช้ในการศึกษาจากแนวทางปฏิบัติที่ดีสำหรับหลักสูตรการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ : กรณีศึกษาของโรงเรียนนายร้อยตำรวจ ได้พบว่า นักเรียนนายร้อยตำรวจกลุ่มตัวอย่างมีทักษะด้านความมั่นคงปลอดภัยไซเบอร์หลังผ่านการเรียนการสอนในหลักสูตรดังกล่าวเพิ่มขึ้นอย่างมีนัยสำคัญ และสามารถสร้างผลงานและแสดงศักยภาพทางด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นที่ประจักษ์ได้ทั้งในระดับเหล่าทัพ ระดับชาติ และระดับนานาชาติ (วงศ์ยศ เกิดศรี, 2564) ทั้งนี้ ผู้เรียนจะต้องฝึกฝนและทดลองเผชิญโจทย์ที่ใกล้เคียงกับสถานการณ์จริงจากการใช้แพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF) ซึ่งเป็นส่วนหนึ่งในกระบวนการจัดการเรียนรู้ความมั่นคงปลอดภัยทางไซเบอร์

บทความนี้จะนำเสนอเรื่องการจัดการเรียนรู้โดยใช้แพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF) ประกอบด้วยรูปแบบการแข่งขัน หมวดหมู่ทักษะการรักษาความมั่นคงปลอดภัยทางไซเบอร์ องค์ประกอบของแพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF) และการเรียนรู้โดยใช้แพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF)

ความหมายของ CTF

การแข่งขันเกมยึดธงทางไซเบอร์ หรือ Capture the Flag (CTF) เป็นเกมการแข่งขันที่ใช้ระบบคอมพิวเตอร์หรือแพลตฟอร์มโฮสต์สภาพแวดล้อมเสมือนจริงสำหรับสอนการรักษาความมั่นคงปลอดภัยไซเบอร์ผ่านประสบการณ์ตรง มีรูปแบบโจทย์ที่มีความยากง่ายแตกต่างกันโดยระดับความยากเป็นตัวกำหนดระยะเวลาที่จะแก้โจทย์ได้สำเร็จ เพื่อพัฒนาความสามารถของผู้เรียน จะมีการแบ่งโจทย์ปัญหาออกเป็น 3 ระดับ ได้แก่ ง่าย

ปานกลาง และยาก ซึ่งจะต้องแก้ปัญหาและดำเนินการตามขั้นตอนให้สำเร็จ ผู้เล่นจะทำทายโจทย์แบ่งตามหมวดหมู่การรักษาความปลอดภัยทางไซเบอร์และทดลองผ่านเครือข่ายห้องปฏิบัติการจำลอง โดยมี 2 ประเภท คือ ด้านเชิงรุกกับด้านเชิงรับ จากนั้นส่งธง (Flag) ซึ่งจะอยู่ในรูปแบบของรหัสหรือข้อความที่ซ่อนอยู่เพื่อรับคะแนน ลำดับคะแนนจะขึ้นอยู่กับความเร็วในการตอบ ทีมที่มีคะแนนมากที่สุดถือเป็นผู้ชนะ (Kucek & Leitner, 2020; Oliveira Júnior et al., 2022; Švábenský et al., 2020; Tirstan et al., 2022; Tann et al., 2023; วงศ์ยศ เกิดศรี, 2564)

แพลตฟอร์มเกมการยึดธงทางไซเบอร์ (CTF Platforms)

แพลตฟอร์มเกมการยึดธงทางไซเบอร์ (CTF Platforms) เป็นนวัตกรรมทางการศึกษาอีกรูปแบบหนึ่งที่นำเทคโนโลยีมาใช้ร่วมกับรูปแบบเกมการแข่งขันเพื่อจัดการเรียนการสอนผ่านอินเทอร์เน็ต ส่งเสริมให้เกิดปฏิสัมพันธ์ระหว่างมนุษย์กับคอมพิวเตอร์ผ่านเครื่องมือการรักษาความปลอดภัยทางไซเบอร์ที่หลากหลายด้วยการใช้ชุดคำสั่ง โปรแกรม และใช้ทักษะการคิดวิเคราะห์แก้ปัญหาในแต่ละโจทย์ สถานการณ์ภัยคุกคามทางไซเบอร์ รวมไปถึงข้อคำถามเกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์อย่างมีจริยธรรม ซึ่งแพลตฟอร์มเกมยึดธงทางไซเบอร์นี้อำนวยความสะดวกให้ผู้เรียนได้ฝึกฝนและทดสอบความสามารถทักษะการรักษาความปลอดภัยทางไซเบอร์ สังเกตประสบการณ์และนำมาประยุกต์ใช้ในชีวิตประจำวัน โดยมีปัจจัยสำคัญในการใช้แพลตฟอร์มเกมยึดธงทางไซเบอร์ในการศึกษาให้สำเร็จ ดังนี้

1. รูปแบบการแข่งขัน

รูปแบบการแข่งขันที่ใช้ในแพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF) มีความยืดหยุ่นในการออกแบบกติกาการแข่งขันและกำหนดให้ผู้เรียนมีปฏิสัมพันธ์ร่วมกันทำงานเป็นทีม มีการแบ่งบทบาทในการเล่น ทั้งนี้จึงควร

จัดเตรียมสภาพแวดล้อมให้ผู้เรียนเตรียมพร้อม เช่น การจัดระบบการลงทะเบียน กติกาการแข่งขัน และหมวดหมู่ของทักษะการรักษาความมั่นคงปลอดภัยทางไซเบอร์ การจัดทีมและวางบทบาทสำหรับการแก้โจทย์ปัญหา โดยรูปแบบการแข่งขันจำนวน 3 รูปแบบ (Karagiannis et al., 2020; Kucek & Leitner, 2020) ดังนี้

1.1 รูปแบบการแข่งขัน Jeopardy

Jeopardy คือ รูปแบบการแข่งขันที่ผู้เข้าร่วมจะแก้ปัญหาในเครื่องคอมพิวเตอร์ของตนหรือโต้ตอบกับเซิร์ฟเวอร์ระยะไกล ผู้เข้าร่วมจะเลือกโจทย์ที่แบ่งออกเป็นหมวดหมู่ต่าง ๆ ซึ่งแต่ละทีมสามารถเข้าถึงโจทย์และดูผลคะแนนพร้อมกันได้ คะแนนแตกต่างกันตามความยากของโจทย์ นอกจากนี้ อาจมีคะแนนโบนัสสำหรับการเป็นคนแรกที่แก้ปัญหาหรือส่งธงได้ซึ่งเรียกว่า “First Blood” และจะถูกเพิ่มเข้ากับคะแนนรวมของทีม ระยะเวลาที่ใช้ในการแข่งขันซึ่งโดยทั่วไปคือ 24 ถึง 48 ชั่วโมง

1.2 รูปแบบการแข่งขัน Attack-Defense

Attack-Defense คือ รูปแบบการแข่งขันที่มีลักษณะการโจมตีเชิงรุกและการป้องกันเชิงรับ โดยทั่วไปแล้วทุกทีมจะเข้าไปในเครือข่ายเครื่องจำลอง ซึ่งแต่ละทีมต้องดูแลรักษาปกป้องเครื่องจำลองฝั่งตนเอง ในขณะที่เดียวกันก็โจมตีหรือใช้ประโยชน์จากช่องโหว่ในการบริการเข้าไปในเครื่องจำลองของทีมตรงข้าม การให้คะแนนขึ้นอยู่กับความสำเร็จในการเข้าถึงและมาตรการรับมือเชิงรับ

1.3 รูปแบบการแข่งขัน King of the Hill

King of Hill คือ รูปแบบการแข่งขันที่มีเครือข่ายเครื่องจำลองเครื่องเดียว มีเป้าหมายหลักคือการยึดระบบเป้าหมายผ่านการตรวจจับช่องโหว่ของระบบและควบคุมให้นานที่สุด โดยผู้เล่นทุกคนโจมตีและป้องกันพร้อมกัน

2. หมวดยุทธศาสตร์การรักษาความปลอดภัยทางไซเบอร์

การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) หรือ มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบภายในประเทศ (สภมช., 2565) มีหมวดยุทธศาสตร์การรักษาความปลอดภัยทางไซเบอร์ มี 2 ด้าน ได้แก่ ทักษะการป้องกัน (Defensive Skill) จะเน้นการปกป้องภัยคุกคามทางไซเบอร์จากการโจมตีของผู้ไม่ประสงค์ดี ซึ่งผู้ปฏิบัติการทางไซเบอร์ด้านป้องกันทางไซเบอร์เชิงรับจะถูกเรียกว่าทีมสีน้ำเงิน (Blue Team) ส่วนทักษะการป้องกัน (Offensive Skill) จะเน้นการโจมตีเจาะระบบและสร้างความเสียหายแก่เครื่องเป้าหมาย ซึ่งผู้ปฏิบัติการด้านการโจมตีทางไซเบอร์เชิงรุกจะถูกเรียกว่า ทีมสีแดง (Red Team) (พายุพิ ศรินาม และ เฉลิมขวัญ ศิริพันธุ์, 2566) โดยมีหมวดยุทธศาสตร์ (Google Inc, 2023; Ortiz-Garcés et al., 2023; Tann et al., 2023; วงศ์ยศ เกิดศรี, 2564)

1. การเขียนโปรแกรม (Programming) เป็นหัวข้อเกี่ยวกับความรู้ด้านการเขียนโปรแกรมในการแก้ปัญหา เช่น การเขียนโปรแกรมขึ้นมาคำนวณหรือจัดการฐานข้อมูลโดยใช้ Python, PHP

2. การเข้าถึงทรัพยากรของเครือข่าย (Network Exploitations) เป็นหัวข้อเกี่ยวกับการใช้ประโยชน์จากช่องโหว่ในโปรโตคอลเครือข่ายและบริการ

3. การเข้าถึงทรัพยากรของเครื่อง (Machine Exploitations) เป็นหัวข้อเกี่ยวกับการเข้าถึงทรัพยากรในเครื่องคอมพิวเตอร์

4. การเข้าถึงทรัพยากรของเว็บ (Web Exploitations) โดยใช้ประโยชน์จากช่องโหว่เว็บไซต์ด้วย

วิธีการต่าง ๆ เช่น SQL Injection, Command Injection, Directory Traversal, Cross Site Scripting

5. การยึดครองควบคุมเครื่อง (Pwnable/ Binary Exploitations) เป็นหัวข้อเกี่ยวกับความปลอดภัยทางไซเบอร์ที่จะค้นหาช่องโหว่ในโปรแกรมและใช้เพื่อควบคุมโปรแกรมที่โต้ตอบผู้ใช้ (Shell) หรือแก้ไขฟังก์ชันของโปรแกรม เช่น การลงทะเบียน (Registers), ชุดลำดับข้อมูล (The Stack), การส่งผ่านอาร์กิวเมนต์และพารามิเตอร์ (Calling Conventions), ตารางเก็บค่าหน่วยความจำและบัฟเฟอร์ข้อมูล (Global Offset Table (GOT) and Buffer)

6. การทำวิศวกรรมย้อนกลับ (Reverse Engineering) เป็นหัวข้อเกี่ยวกับการคอมไพล์โปรแกรมรหัสเครื่อง รูปแบบไฟล์ Binary แล้วแปลงมันเป็นรูปแบบที่มนุษย์สามารถอ่านได้มากขึ้น เช่น ภาษาแอสเซมบลี ภาษาซี โปรแกรมแปลภาษาเครื่องหรือภาษาปลายทาง

7. การตรวจพิสูจน์ทางดิจิทัล (Digital Forensics) เป็นหัวข้อเกี่ยวกับการพิสูจน์หลักฐาน รวมไปถึงการวิเคราะห์รูปแบบไฟล์ เช่น วิทยาการอำพรางข้อมูล (Steganography) การวิเคราะห์การถ่ายโอนข้อมูลหน่วยความจำ (Memory Dump) หรือ วิเคราะห์การจับแพ็กเก็ตเครือข่าย (Network Packet Capture) การวิเคราะห์ภัยคุกคามบนระบบ (Sandboxing)

8. วิทยาการเข้ารหัสลับ (Cryptography) เป็นหัวข้อเกี่ยวกับโครงสร้างรูปแบบวิธีการสร้างข้อมูล การเข้ารหัสและถอดรหัสข้อมูล เช่น XOR, Caesar Cipher, Substitution Cipher, Vigenere Cipher, Hashing Functions, Block Ciphers, Stream Ciphers, and RSA

9. การใช้เครื่องมือข่าวกรองทางแหล่งข้อมูลเปิด (OSINT) หมวดยุทธศาสตร์เน้นการเพื่อรวบรวมข้อมูลเกี่ยวกับเป้าหมายก่อนโจมตี เช่น การเดารหัสผ่านจากข้อมูลบนเว็บไซต์ การสร้างอีเมลปลอมเพื่อได้มาซึ่งข้อมูลของเป้าหมาย

10. ความรู้เบ็ดเตล็ด (Miscellaneous) เป็นหมวดอื่น ๆ เน้นการตามหาข้อมูลที่ซ่อนอยู่ในโลกออนไลน์หรือหาข้อมูลที่ซ่อนอยู่จากโจทย์ที่กำหนด เช่น การวิเคราะห์ไฟล์เสียง การวิเคราะห์ไฟล์ภาพ

11. การรักษาความปลอดภัยบนอุปกรณ์เคลื่อนที่ (Mobile Security) เป็นหัวข้อเน้นการตรวจสอบความปลอดภัยเบื้องต้นของแอปพลิเคชันบนมือถือทั้งระบบปฏิบัติการ Android และ iOS โดยเน้นสิทธิการเข้าถึงระบบ

องค์ประกอบของแพลตฟอร์มเกมยึดตรงทางไซเบอร์ (CTF)

องค์ประกอบแพลตฟอร์มเกมยึดตรงทางไซเบอร์ (CTF) มี 4 อย่าง (Ortiz-Garcés et al., 2023; Swann et al., 2021) ประกอบด้วย

1. ส่วนหลักของแพลตฟอร์มเกมยึดตรงทางไซเบอร์ CTF (Main) ซึ่งมีการนำเสนอคำแนะนำการแข่งขันและประเภทต่าง ๆ ที่มีอยู่ โดยแสดงชื่อผู้ใช้แต่ละคน ชื่อทีม คะแนน คำอธิบาย คำใบ้ และเอกสารแนบบนโจทย์ และมีช่องทางส่งธงเพื่อตอบโจทย์

2. ป้ายคะแนน (Scoreboard) ส่วนนี้จะนำเสนอคะแนนทั้งทีมและรายบุคคลระหว่างการแข่งขัน

3. พื้นที่เก็บข้อมูล (Writeups) เป็นส่วนเก็บข้อมูลพื้นฐานและโจทย์ปัญหาผ่านลิงก์นำเสนอพื้นที่การเรียนรู้ โดยแบ่งออกเป็นหมวดหมู่และระดับความยาก ในช่วงเริ่มต้นของการแข่งขันแต่ละครั้ง โจทย์พื้นฐานหรือข้อง่ายจะถูกเปิดใช้งานและในขณะที่ผู้เรียนทำโจทย์ ระดับกลางและระดับยากจะถูกเปิดใช้งาน แต่ละหมวดหมู่ประกอบด้วยทรัพยากรที่ต้องใช้ทั้งความรู้ ทฤษฎี และทักษะการปฏิบัติการทางไซเบอร์

4. การแสดงสรุปผล (Dashboard) พื้นที่รายงานข้อมูลและผลลัพธ์กิจกรรมบนแพลตฟอร์มที่ผ่านมาทั้งหมด อีกทั้งใช้เพื่อสำรองข้อมูลเป็นรายงานเพื่อตรวจสอบการเรียนรู้ของผู้เรียน

ตัวอย่างแพลตฟอร์มเกมยึดตรงทางไซเบอร์

จากการศึกษาแพลตฟอร์มเกมยึดตรงทางไซเบอร์ที่เป็นที่นิยมและใช้ส่งเสริมการเรียนรู้มีหลากหลายแพลตฟอร์มด้านการศึกษา รวมทั้งแพลตฟอร์มการแข่งขัน เช่น

1. แพลตฟอร์มเกมยึดตรงทางไซเบอร์ทางการศึกษา

1.1 Facebook CTF หรือ FBCTF ได้รับการพัฒนาโดยวิศวกรระบบรักษาความปลอดภัยของ Facebook เพื่อให้มีความสะดวกในการจัดการแข่งขัน CTF ซึ่งง่ายต่อการติดตั้งเครื่องโฮสต์ด้วยรูปแบบการแข่งขัน Jeopardy หรือ King of the Hill โดยออกแบบคำนึงถึงความยืดหยุ่นและการเชื่อมต่อทรัพยากรเครื่องขึ้นอยู่กับความต้องการของผู้ใช้ แพลตฟอร์ม FBCTF มีการออกแบบกราฟิกดึงดูดความสนใจในรูปแบบของแผนที่โลกและเมืองประกอบของเกม อีกทั้งรองรับการใช้งานหลายภาษา (Karagiannis et al., 2020; Kucek & Leitner, 2020; Ortiz-Garcés et al., 2023)

1.2 CTFd เป็นแพลตฟอร์มเครื่องมือแบบฟรีแวร์ (Freeware) ที่พัฒนาบนระบบเว็บเพื่อตอบสนองความต้องการของ Cyber Security Awareness ทั่วโลก และถือเป็นหนึ่งใน CTF ที่เก่าแก่และใหญ่ที่สุดซึ่งเรียกว่า CSAW หรือ กิจกรรมด้านความปลอดภัยทางไซเบอร์ ที่ออกแบบมาเพื่ออำนวยความสะดวกในการใช้งานของทั้งผู้ดูแลระบบและผู้ใช้ นอกจากนี้ยังมีฟังก์ชันที่ช่วยให้จัดการแข่งขัน เนื่องจากเป็น Open-Source ทำให้ง่ายต่อการติดตั้งและแก้ไข นอกจากนี้แพลตฟอร์มนี้มุ่งเน้นไปที่การนำเสนอข้อมูลและรายงานผลทางสถิติ (Karagiannis et al., 2020; Kucek & Leitner, 2020; Ortiz-Garcés et al., 2023)

1.3 HackTheBox หรือ HTB เป็นแพลตฟอร์มที่ได้รับการอนุญาตในการสร้างรูปแบบการฝึกอบรมความปลอดภัยทางไซเบอร์แบบออนไลน์ขนาดใหญ่ที่เปิดโอกาสให้บุคคล บริษัท มหาวิทยาลัย และองค์กรทุกภาคส่วนสามารถพัฒนาทักษะการรักษาความปลอดภัยทางไซเบอร์ ในแพลตฟอร์มการเรียนรู้มี HTB Academy สำหรับการแข่งขัน CTF และสำหรับฝึกผ่านสภาพแวดล้อมที่มีการควบคุมด้วยแพลตฟอร์ม Wargame ชื่อว่า Hack The Box โดยสามารถสมัครใช้งาน เมื่อทำการแก้ไขภัยในแพลตฟอร์มจะได้คะแนน CPE (Continuing Professional Education) ซึ่งสามารถนำไปต่ออายุใบรับรองในระดับสากลขององค์กรด้านการฝึกอบรมและการรับรองสำหรับผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ (ISC)² ทั้งนี้ จากกระแสนี้ คณะกรรมการระดับโลกสำหรับทีมทั่วโลกที่เผยแพร่มีหลายบริษัทนำผลคะแนนไปใช้ในการคัดเลือกพนักงานใหม่ (พิชญะ โมริโมโต, 2563; Ortiz-Garcés et al., 2023)

1.4 TryHackMe หรือ THM เป็นแพลตฟอร์มที่สอนความปลอดภัยทางไซเบอร์โดยใช้ห้องปฏิบัติการเสมือนจริงขนาดเล็กที่จำลองมาจากสถานการณ์จริง มีเนื้อหาสำหรับทั้งผู้เริ่มต้นและนักวิทยาการคอมพิวเตอร์ที่มีประสบการณ์ นอกจากนี้ยังมีคำแนะนำและความท้าทายเพื่อตอบสนองรูปแบบการเรียนรู้ที่แตกต่างกัน (Ortiz-Garcés et al., 2023)

2. แพลตฟอร์มรายการแข่งขันเกมยึดธงทางไซเบอร์

2.1 การแข่งขันทักษะทางไซเบอร์กองทัพไทย ประจำปี 2566 ระดับกองทัพไทย และระดับโรงเรียนทหาร-ตำรวจ และอุดมศึกษา “RTARF CYBER WARRIOR CONTEST 2023 หรือ RTATF CWC” โดยเป็นการแข่งขันที่จัดขึ้นเพื่อพัฒนาขีดความสามารถด้านไซเบอร์ของประเทศ โดยมีหน่วยงานที่เข้าร่วม จำนวน 78 ทีม รวมทั้งมีทีมจากต่างประเทศ มีรูปแบบการเล่นจำนวน 10 หมวดหมู่ทักษะการรักษาความปลอดภัยทางไซเบอร์ เงินรางวัลมูลค่ากว่า 140,000 บาท (CTF Thailand, 2566a)

2.2 การแข่งขัน Thailand Cyber Top Talent 2023 หรือ TCTT เป็นการแข่งขันด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย จัดโดย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ร่วมกับ บริษัท หัวเว่ย เทคโนโลยี (ประเทศไทย) จำกัด โดยเป็นการแข่งขันที่จัดขึ้นเพื่อมุ่งหวังให้นักเรียน นิสิต นักศึกษา และประชาชนทั่วไปที่เข้าร่วมได้เรียนรู้พัฒนาทักษะและประสบการณ์เพื่อให้กลายเป็นบุคลากรที่มีความรู้ความสามารถด้านความมั่นคงปลอดภัยไซเบอร์และเป็นการสร้างแรงงานออกสู่ตลาดแรงงานในอนาคต อีกทั้งเป็นการช่วยเพิ่มความตระหนักรู้เกี่ยวกับภัยคุกคามทางด้านไซเบอร์ให้กับบุคคลทั่วไปมากขึ้น และผู้ที่ได้รับรางวัลชนะเลิศ ยังมีสิทธิเป็นตัวแทนประเทศไทยไปแข่งขันในรายการ Cyber SEA Game 2023 โดยมีรางวัลรวมทั้ง 3 รายการกว่า 450,000 บาท (CTF Thailand, 2566b)

2.3 การแข่งขัน Google CTF 2023 เป็นการแข่งขันทั่วโลกโดยแบ่งออกเป็น 2 ส่วน ได้แก่ การแข่งขัน Jeopardy-CTF ออนไลน์ และการแข่งขันในสถานที่อื่น เปิดให้เฉพาะทีม 8 อันดับแรกของการแข่งขันเท่านั้น การแข่งขัน Capture The Flag (CTF) ประกอบด้วยชุดโจทย์ด้านการรักษาความปลอดภัยทางไซเบอร์ที่เกี่ยวข้องกับวิศวกรรมย้อนกลับ หน่วยความจำข้อมูล การเข้ารหัส เทคโนโลยีเว็บไซต์ และอื่น ๆ เมื่อผู้เล่นไขปริศนาได้จะได้รับ “ธง” ซึ่งเป็นข้อมูลลับที่สามารถแลกเป็นคะแนนได้ ยิ่งทีมได้รับคะแนนมากเท่าใด อันดับก็จะยิ่งสูงขึ้นเท่านั้น ทีม 3 อันดับแรกจาก CTF Jeopardy จะได้รับรางวัล 12,000, 5,000 และ 3,000 ดอลลาร์สหรัฐ และทีม 8 อันดับแรกจะได้รับเชิญให้เข้าร่วมการแข่งขันอีกครั้งเพื่อแข่งขันชิงรางวัลเพิ่มเติมสูงสุดถึง 7,000 ดอลลาร์สหรัฐ โดยแต่ละโจทย์จะมีค่าลับหรือธง (Flag) ที่มีรูปแบบ CTF {some-secret-value-here} ซึ่งใช้ในการส่งเพื่อรับคะแนน (Google Inc, 2023)

การจัดการเรียนรู้โดยใช้แพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF)

การจัดการเรียนรู้โดยใช้แพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF) มีบทความและงานวิจัยที่เกี่ยวข้องกับการนำแพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF) ไปใช้เพื่อส่งเสริมทักษะการรักษาความปลอดภัยทางไซเบอร์ทั้งในระบบคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ในระดับอุดมศึกษา ดังนี้

ผลการวิจัย การใช้โมเดลภาษาขนาดใหญ่ (Large Language Models: LLM) สำหรับการแข่งขันเกมยึดธงทางไซเบอร์ (CTF) และช่วยให้ผ่านใบรับรองทางไซเบอร์พบว่า การใช้แบบจำลองภาษาขนาดใหญ่เพื่อตอบคำถามการรับรองจากผู้เชี่ยวชาญและแก้ปัญหาโจทย์บนแพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF) โดยประเมินความสามารถในการตอบคำถามของ LLM ในระดับต่าง ๆ ตามการรับรองของ Cisco เพื่อวัดประสิทธิภาพของคำถามประเภทต่าง ๆ ผู้วิจัยใช้ LLM ได้แก่ OpenAI-ChatGPT, Google Bard และ Microsoft Bing กับการทดสอบโจทย์ CTF จำนวน 5 หมวดหมู่และตรวจสอบว่าแบบฝึกหัด CTF มีประโยชน์อย่างไรในห้องเรียน ผลการวิจัย พบว่า ChatGPT สามารถตอบคำถามตามการรับรองทางวิชาชีพ ซึ่งเป็นคำถามข้อเท็จจริงได้แม่นยำกว่าคำถามเชิงแนวคิด โดย ChatGPT ตอบคำถามปรนัยที่เป็นข้อเท็จจริงได้อย่างถูกต้องมากที่สุดถึงร้อยละ 82 และจากโจทย์บนแพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF) ที่ผู้ใช้ได้รับความช่วยเหลือจาก AI ที่ LLM สร้างขึ้น มีแนวทางแก้ไขซึ่งให้ข้อได้เปรียบสำคัญในแข่งขันเกมยึดธงทางไซเบอร์ (CTF) จากมีผู้เรียนเข้าร่วม 50 คน มีผู้เรียนประมาณ 40 คนที่สามารถพัฒนาทักษะภายในหนึ่งเดือนบนแพลตฟอร์ม CTF-PCT ที่ผู้วิจัยสร้างขึ้นคิดเป็นร้อยละ 80 อีกทั้งผู้เข้าร่วมสังเกตเห็นการเพิ่มขึ้นด้านวิชาการและความก้าวหน้านับตั้งแต่เริ่มการแข่งขันทั้งนี้การแข่งขันเกมยึดธงทางไซเบอร์ (CTF) มีส่วนสำคัญ

ในการขับเคลื่อนการพัฒนาทักษะด้านการรักษาความปลอดภัยทางไซเบอร์และเป็นพื้นที่แสดงให้เห็นถึงการบรรลุความสำเร็จและในปัจจุบันถูกมองว่าเป็นรากฐานของอนาคต (Tann et al., 2023)

ผลการวิจัย การพัฒนาแพลตฟอร์มเพื่อการเรียนรู้การรักษาความปลอดภัยทางไซเบอร์จากการใช้เกมยึดธงทางไซเบอร์ พบว่า การประเมินผลประกอบด้วยโจทย์จำนวน 5 ข้อคำถาม สำหรับแต่ละระดับ และมีผู้เข้าร่วม 22 คน เมื่อเข้าสู่พื้นที่การเรียนรู้ ผู้เรียนจะตอบคำถามแต่ละลำดับและจะค่อย ๆ เปิดหมวดหมู่อื่นเพิ่มขึ้นจนครบจำนวน 5 หมวดหมู่ แต่ละครั้งที่ผู้เรียนเรียนจบในแต่ละหมวดหมู่ จะมีการนำเสนอโจทย์ข้อคำถามผลการประเมินพบว่า ค่าเฉลี่ย ผู้เรียนมีพัฒนาการดีขึ้นร้อยละ 24.78 ด้วยผลลัพธ์นี้สามารถตรวจสอบได้ว่าแม้ผู้เรียนจะมีความรู้ด้านความปลอดภัยทางไซเบอร์มาก่อนแล้วสามารถเพิ่มระดับให้สูงขึ้นได้ โดยในระหว่างการแข่งขัน ได้มีการลงมติการสำรวจการใช้งานของแพลตฟอร์มซึ่งเป็นส่วนหนึ่งของเกมยึดธงทางไซเบอร์ (CTF) โดยมีผลการสำรวจการเข้าถึงและการใช้งานแพลตฟอร์มจากผู้เข้าร่วมทั้งหมด 22 คน พบว่า มีผู้เรียนเพียง 1 คนที่พบว่า การใช้งานและการโต้ตอบกับแพลตฟอร์มได้ยากนอกจากนี้ผู้เรียนร้อยละ 55 เสนอว่า แพลตฟอร์มนั้นง่ายต่อการใช้งาน ขณะที่ร้อยละ 40 ของผู้เรียนถือว่าการใช้งานแพลตฟอร์มเป็นเรื่องปกติ จึงถือเป็นการจัดการเรียนรู้ที่เป็นประโยชน์ก่อนการพัฒนาความสามารถ นอกจากนี้การออกแบบแพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF) มีเพื่อให้ผู้เรียนสนใจและตระหนักถึงการรักษาความปลอดภัยทางไซเบอร์ จากแบบสำรวจความสนใจของผู้เรียนแต่ละคนเกี่ยวกับความปลอดภัยทางไซเบอร์หลังจากใช้แพลตฟอร์ม พบว่า ผู้เรียนร้อยละ 90 มีความสนใจการรักษาความปลอดภัยทางไซเบอร์เนื่องจากการใช้แพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF) และเนื้อหามีความเหมาะสม (Ortiz-Garcés et al., 2023)

ผลการวิจัย แนวทางปฏิบัติที่สำคัญสำหรับหลักสูตร การเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ : กรณีศึกษาของโรงเรียนนายร้อยตำรวจ พบว่า นักเรียน นายร้อยตำรวจกลุ่มตัวอย่างจำนวน 40 คน มีผลคะแนน เกินกว่าร้อยละ 60 ทุกคน คิดเป็นร้อยละ 100 ของจำนวน ผู้ที่ผ่านการประเมิน โดยนักเรียนนายร้อยตำรวจกลุ่มตัวอย่าง ที่มีความถนัดในด้านความมั่นคงปลอดภัยไซเบอร์เชิงรุก จำนวน 12 คน มีความถนัดในด้านความมั่นคงปลอดภัย ไซเบอร์เชิงรับจำนวน 25 คน และมีความถนัดทั้งสองด้าน จำนวน 3 คน โดยเนื้อหาที่นักเรียนนายร้อยตำรวจ กลุ่มตัวอย่างมีความถนัดมากที่สุดคือ เนื้อหาเรื่องการ ตรวจพิสูจน์ทางดิจิทัล (Digital Forensic) และวิทยาการ เข้ารหัสลับ (Cryptography) แสดงให้เห็นว่า ผู้เรียน มีทักษะทางด้านความมั่นคงปลอดภัยไซเบอร์เพิ่มมากขึ้น โดยสามารถทำคะแนนได้มากกว่าร้อยละ 80 เป็น จำนวนเพิ่มขึ้นจากกรอบที่ 1 นอกจากนี้ผลการสอน ด้านความมั่นคงปลอดภัยไซเบอร์ทำให้นักเรียนนายร้อย ตำรวจกลุ่มตัวอย่างมีโอกาสได้เข้าร่วมการแข่งขันทักษะ

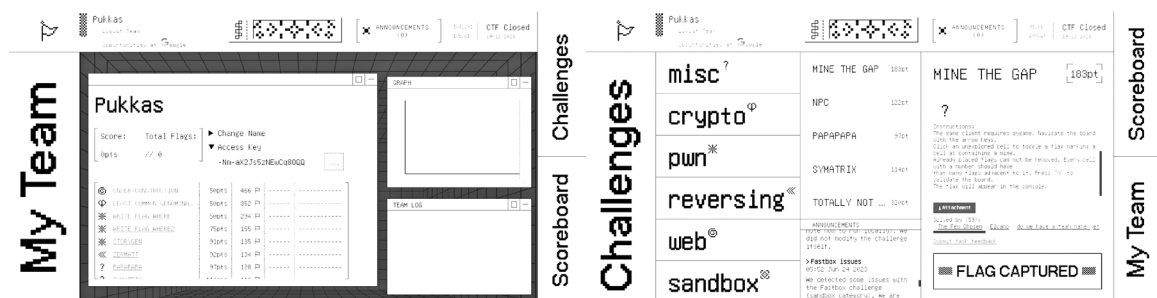
ทางไซเบอร์ในระดับชาติและทำผลงานได้เป็นที่ประจักษ์ จากการแข่งขันรายการต่าง ๆ ทั้งในประเทศและต่างประเทศ (วงศ์ยศ เกิดศรี, 2564)

การศึกษาการจัดการเรียนรู้โดยใช้แพลตฟอร์ม เกมยึดธงทางไซเบอร์ (CTF) แสดงให้เห็นว่าการใช้แพลตฟอร์ม เกมยึดธงทางไซเบอร์ (CTF) เป็นปัจจัยสำคัญในการพัฒนา ความสามารถและทักษะด้านการรักษาความปลอดภัย ทางไซเบอร์ซึ่งมีความสำคัญในยุคปัจจุบัน อีกทั้งมีความ หลากหลายของหมวดหมู่ที่ให้ผู้เรียนได้พัฒนา ความถนัดแตกต่างกันในด้านการรักษาความปลอดภัย ทางไซเบอร์เชิงรุกและเชิงรับ รวมไปถึงทักษะการแก้ปัญหา การทำงานเป็นทีมและการใช้เครื่องมือต่าง ๆ ในการ แก้ไขภัยคุกคามองค์ความรู้จากการศึกษา

การศึกษาเกี่ยวกับแพลตฟอร์มเกมยึดธงทางไซเบอร์ ที่มีหัวข้อหมวดหมู่ทักษะการรักษาความปลอดภัยทางไซเบอร์ องค์ประกอบแพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF) และการจัดการเรียนรู้โดยใช้แพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF) มีผลการศึกษาค้นคว้ามดังในภาพที่ 1 และตารางที่ 1

ภาพ

หน้าปายคะแนนการแข่งขัน Google CTF 2023 และหมวดหมู่การรักษาความมั่นคงปลอดภัยทางไซเบอร์



หมายเหตุ : จาก Google Ctf, by Google Inc., 2023 (<https://capturetheflag.withgoogle.com/>)

ตาราง

สังเคราะห์หมวดหมู่ทักษะการรัรักษาความปลอดภัยทางไซเบอร์จากแพลตฟอร์มฯ

ระบบการใช้ CTF		เครือข่ายท้องถิ่น	เครือข่ายท้องถิ่น	เครือข่ายท้องถิ่น	เครือข่ายท้องถิ่น	ห้องปฏิบัติการเสมือน	ห้องปฏิบัติการเสมือน	การแข่งขันไลน์	การแข่งขันไลน์	การแข่งขันไซต์
อ้างอิง		วงศ์ยศ เกิดศรี (2564)	Tann et al. (2023)	Ortiz-Garcés et al. (2023)				CTF Thailand (2066b)	Google Inc (2023)	(CTF) Thailand, 2566a)
หมวดหมู่/แพลตฟอร์ม		CTFd	CTFd	CTFd	FBCTF	HTB	THM	TCTT	Google CTF	RTAF CWC
ด้านความมั่นคงปลอดภัยไซเบอร์เชิงรุก	1. การเขียนโปรแกรม (Programming)	✓		✓	✓		✓	✓		✓
	2. การเข้าถึงทรัพยากรของเครือข่าย (Network Exploitations)	✓						✓		✓
	3. การเข้าถึงทรัพยากรของเครื่อง (Machine Exploitations)	✓								
	4. การเข้าถึงทรัพยากรของเว็บ (Web Exploitations)	✓	✓	✓	✓	✓	✓	✓	✓	✓
	5. การยึดครองควบคุมเครื่อง (Pwnable/Binary Exploitations)	✓	✓	✓	✓	✓	✓	✓	✓	✓
ด้านความมั่นคงปลอดภัยไซเบอร์เชิงรับ	6. การทำวิศวกรรมย้อนกลับ (Reverse Engineering)	✓	✓	✓	✓	✓	✓	✓	✓	✓
	7. การตรวจพิสูจน์ทางดิจิทัล (Digital Forensics)	✓	✓	✓	✓	✓	✓	✓	✓	✓
	8. วิทยาการเข้ารหัสลับ (Cryptography)	✓	✓	✓	✓	✓	✓	✓	✓	✓
	9. การใช้เครื่องมือข่าวกรองทางแหล่งข้อมูลเปิด (OSINT)	✓		✓	✓					
	10. ความรู้เบ็ดเตล็ด (Miscellaneous)	✓		✓	✓	✓			✓	✓
	11. การรักษาความปลอดภัยบนอุปกรณ์เคลื่อนที่ (Mobile Security)			✓	✓	✓		✓		✓

จากผลการศึกษา ผู้เรียนจะพัฒนาทักษะการใช้เครื่องมือการรักษาความมั่นคงทางไซเบอร์ผ่านการจัดการเรียนรู้ด้วยแพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF) ซึ่งเป็นการจำลองยุทธทางไซเบอร์ที่ให้ผู้เรียนได้ทำงานผ่านโจทย์ที่น่าท้าทายหลายอย่างโดยใช้เทคโนโลยีทางไซเบอร์และใช้เครื่องมือเทคโนโลยี AI ได้อย่างสร้างสรรค์และมีจริยธรรม ทั้งนี้จากการสังเคราะห์ พบว่า แพลตฟอร์ม CTFd ที่ติดตั้งบนเครือข่ายท้องถิ่นมีการใช้งานมากที่สุด เนื่องจากมีความยืดหยุ่นในการกำหนดหมวดหมู่ และภาพรวมหมวดหมู่ที่ใช้บนแพลตฟอร์ม CTFd ประกอบด้วย ทักษะการรักษาความปลอดภัยทางไซเบอร์ 2 ด้าน ได้แก่ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เชิงรุก ซึ่งหมวดหมู่ที่มักใช้ในเกมการแข่งขันมากที่สุด 3 หมวดหมู่ ได้แก่ การเขียนโปรแกรม (Programming) การเข้าถึงทรัพยากรของเว็บ (Web Exploitations) และการยึดครองควบคุมเครื่อง (Pwnable/Binary Exploitations) ส่วนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เชิงรับ มีหมวดหมู่ที่มักใช้ในการแข่งขันมากที่สุด 3 หมวดหมู่ ได้แก่ การทำวิศวกรรมย้อนกลับ (Reverse Engineering) การตรวจพิสูจน์ทางดิจิทัล (Digital Forensics) และ วิทยาการเข้ารหัสลับ (Cryptography)

แพลตฟอร์มที่เหมาะสมในการฝึกโจทย์ในเครื่องจำลองหรือห้องปฏิบัติการเสมือนจริง ได้แก่ Hack The Box และ Try Hack Me ซึ่งมีหมวดหมู่ที่มีการเน้นเหมือนกัน 5 หมวดหมู่ คือ การเข้าถึงทรัพยากรของเว็บ (Web Exploitations) การยึดครองควบคุมเครื่อง (Pwnable/Binary Exploitations) การทำวิศวกรรมย้อนกลับ (Reverse Engineering) การตรวจพิสูจน์ทางดิจิทัล (Digital Forensics) วิทยาการเข้ารหัสลับ (Cryptography) แพลตฟอร์มเกมยึดธงทางไซเบอร์ที่ใช้ในการแข่งขันจะมีหมวดหมู่ทั้งหมด 10 หมวดหมู่ ได้แก่ 1) การเขียนโปรแกรม (Programming) 2) การเข้าถึงทรัพยากรของเครือข่าย

(Network Exploitations) 3) การเข้าถึงทรัพยากรของเว็บ (Web Exploitations) 4) การยึดครองควบคุมเครื่อง (Pwnable/Binary Exploitations) 5) การทำวิศวกรรมย้อนกลับ (Reverse Engineering) 6) การตรวจพิสูจน์ทางดิจิทัล (Digital Forensics) 7) วิทยาการเข้ารหัสลับ (Cryptography) 8) การใช้เครื่องมือข่าวกรองทางแหล่งข้อมูลเปิด (OSINT) 9) ความรู้เบ็ดเตล็ด (Miscellaneous) 10) การรักษาความปลอดภัยบนอุปกรณ์เคลื่อนที่ (Mobile Security)

บทสรุป

สรุปในภาพรวมของบทความ การจัดการเรียนรู้โดยใช้แพลตฟอร์มเกมยึดธงทางไซเบอร์ (CTF) จะมีรูปแบบการแข่งขันเกมยึดธงทางไซเบอร์ (CTF) 3 รูปแบบ คือ Jeopardy, Attack-Defense และ King of the Hill และมีหมวดหมู่ทักษะการรักษาความปลอดภัยทางไซเบอร์ 2 ด้าน ประกอบด้วย ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เชิงรุกและด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เชิงรับ ซึ่งมีหมวดหมู่ที่นิยมใช้บนแพลตฟอร์มเกมยึดธงทางไซเบอร์สำหรับฝึกฝนและในการแข่งขัน 10 หมวดหมู่ ได้แก่ การเขียนโปรแกรม (Programming) การเข้าถึงทรัพยากรของเครือข่าย (Network Exploitations) การเข้าถึงทรัพยากรของเว็บ (Web Exploitations) การยึดครองควบคุมเครื่อง (Pwnable/Binary Exploitations) การทำวิศวกรรมย้อนกลับ (Reverse Engineering) การตรวจพิสูจน์ทางดิจิทัล (Digital Forensics) วิทยาการเข้ารหัสลับ (Cryptography) การใช้เครื่องมือข่าวกรองทางแหล่งข้อมูลเปิด (OSINT) ความรู้เบ็ดเตล็ด (Miscellaneous) การรักษาความปลอดภัยบนอุปกรณ์เคลื่อนที่ (Mobile Security) โดยมีแพลตฟอร์มที่เป็นที่นิยมใช้ในการออกแบบการแข่งขันมากที่สุด คือ CTFd การจัดการเรียนรู้โดยใช้แพลตฟอร์มเกมยึดธง

ทางไซเบอร์ (CTF) จึงเป็นเครื่องมือในการประเมินผลทักษะ การรักษาความปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพ และเป็นปัจจัยสำคัญในการพัฒนาความสามารถและทักษะ ด้านการรักษาความปลอดภัยทางไซเบอร์ ที่มีหมวดหมู่ หลากหลายด้านให้ผู้เรียนได้พัฒนาความถนัดแตกต่างกัน ในด้านการรักษาความปลอดภัยทางไซเบอร์เชิงรุกและเชิงรับ รวมไปถึงทักษะการแก้ปัญหาการทำงานเป็นทีม และการใช้ เครื่องมือต่าง ๆ ในการแก้โจทย์ปัญหา ทั้งนี้ในการจัด การเรียนรู้จะต้องคำนึงถึงความซับซ้อนในการออกแบบ โจทย์และระบบการแข่งซึ่งต้องอาศัยผู้เชี่ยวชาญ ความต้องการทรัพยากรทางเทคโนโลยีที่เพียงพอ เช่น เครือข่าย เครื่องเซิร์ฟเวอร์ และระบบรักษาความปลอดภัย

อีกทั้งผู้เรียนบางส่วนอาจพบว่ายากเกินไป หากไม่มีพื้นฐานมาก่อน จึงต้องมีการจัดลำดับความยากและ การสนับสนุนที่เหมาะสม ดังนั้นจึงควรประยุกต์ใช้ CTF ทั้งในหลักสูตรการเรียนการสอนและการพัฒนาศักยภาพ บุคลากร การบูรณาการในรายวิชาระดับมัธยมศึกษา อุดมศึกษา การจัดเป็นกิจกรรมเสริมสร้างความตระหนักรู้ ในชุมชนดิจิทัล นอกจากนี้การออกแบบโจทย์ควรมี ความต่อเนื่องและหลากหลาย โดยเริ่มจากระดับพื้นฐาน ไปจนถึงขั้นสูงเพื่อรองรับผู้เรียนที่มีความแตกต่างด้านพื้นฐาน ความรู้ อีกทั้งควรพิจารณาสร้างความร่วมมือกับหน่วยงาน ที่เกี่ยวข้องเพื่อพัฒนาแพลตฟอร์มที่เหมาะสมกับบริบทไทย และสร้างระบบสนับสนุนให้ผู้เรียนเข้าถึงได้อย่างทั่วถึง

เอกสารอ้างอิง

- พายัพ ศิรินาม และเฉลิมขวัญ ศิริพันธุ์. (2566). การพัฒนาโจทย์สถานการณ์สำหรับแบบจำลองยุทธทางไซเบอร์ ของกองทัพอากาศ. *วารสารวิชาการการประยุกต์ใช้เทคโนโลยีสารสนเทศ*, 9(1), 23-41. <https://ph02.tci-thaijo.org/index.php/project-journal/article/view/248726>
- พิชญะ โมริโมโต. (2563, 4 ธันวาคม). *ยกระดับศักยภาพของทีม IT Security องค์กรด้วยการเล่น CTF*. NT cyfence. <https://www.cyfence.com/article/empower-your-itsecurity-team-with-capture-the-flag/>
- วงศ์ยศ เกิดศรี. (2564). แนวทางปฏิบัติที่ดีสำหรับหลักสูตรการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์: กรณีศึกษา ของโรงเรียนนายร้อยตำรวจ. *วารสารอาชีวศึกษาและนิติวิทยาศาสตร์*, 7(2), 136-150. <https://so02.tci-thaijo.org/index.php/forensic/article/view/250248>
- สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2565, 9 ธันวาคม). *นโยบายและแผนปฏิบัติการว่า ด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570)*. <https://drive.ncsa.or.th/s/5RFcH5MmgmJgGtR>
- สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ. (2562). *สรุปผลการสำรวจข้อมูลสถานการณ์การรู้เท่าทันสื่อและสารสนเทศของประเทศไทย ปี พ.ศ. 2562*. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2562). *รายงานผลการสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2561*. <https://www.etda.or.th/th/Useful-Resource/publications/Thailand-Internet-User-Behavior-2018.aspx>
- Capture the Flag Thailand. (2566a, 9 กรกฎาคม). *การแข่งขันทักษะทางไซเบอร์กองทัพไทย ประจำปี 2566 ระดับกองทัพไทย และระดับโรงเรียนทหาร-ตำรวจ และอุดมศึกษา*. <https://ctf.in.th/news/2224/>

- Capture the Flag Thailand. (2566b, 19 กรกฎาคม). *การแข่งขัน Thailand Cyber Top Talent 2023*. <https://ctf.in.th/challenge/2254/>
- Google Inc. (2023, June 25). *Google Ctf*. <https://capturetheflag.withgoogle.com/>
- International Telecommunication Union. (2018). *Measuring the information society report 2018*. <https://www.itu.int/en/ITU-D/Statistics/pages/publications/misr2018.aspx>
- Karagiannis, S., Maragkos-Belmpas, E., & Magkos, E. (2020). An analysis and evaluation of open source capture the flag platforms as cybersecurity e-learning tools. In L. Drevin, S. Von Solms, & M. Theocharidou (Eds.), *Information Security Education. Information Security in Action* (pp. 61-77). Springer, Cham. https://doi.org/10.1007/978-3-030-59291-2_5
- Kucek, S., & Leitner, M. (2020). An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments. *Journal of Network and Computer Applications*, 151, 102470. <https://doi.org/10.1016/j.jnca.2019.102470>
- Oliveira Júnior, A., Funchal, G., Queiroz, J., Loureiro, J., Pedrosa, T., Dominguez, J., & Leitão, P. (2022). *Learning Cybersecurity in IoT-based Applications through a Capture the Flag Competition*. <https://doi.org/10.1109/INDIN51773.2022.9976079>
- Ortiz-Garcés, I., Gutierrez, R., Guerra, D., Sanchez-Viteri, S., & Villegas, W. (2023). Development of a Platform for Learning Cybersecurity Using Capturing the Flag Competitions. *Electronics*, 12, 1753. <https://doi.org/10.3390/electronics12071753>
- Švábenský, V., Celeda, P., Vykopal, J., & Brisakova, S. (2020). Cybersecurity Knowledge and Skills Taught in Capture the Flag Challenges. *Computers & Security*, 102, 102154. <https://doi.org/10.1016/j.cose.2020.102154>
- Swann, M., Rose, J., Bendiab, G., Shiaeles, S., & Li, F. (2021). Open source and commercial capture the flag cyber security learning platforms - A case study. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. <https://doi.org/10.1109/CSR51186.2021.9527941>
- Tirstan, J., Gilbert, J. A., & Nelmiawati, N. (2022). Analysis of cyber security knowledge and skills for capture the flag competition. *Jurnal Integrasi*, 14(1), 14-22. <https://doi.org/10.30871/ji.v14i1.3986>
- Tann, W., Liu, Y., Sim, J., Seah, C., & Chang, E.-C. (2023). *Using large language models for cybersecurity capture-the-flag challenges and certification questions*. arXiv. <https://arxiv.org/abs/2308.10443>