สัมมนาวิชาการ เทคโนโลยีดิจิทัลมีเดีย ระดับบัณฑิตศึกษา ครั้งที่ 3

การจำลองสภาพแวดล้อมอัจฉริยะสำหรับการวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ในประเทศไทย

An Intelligent Simulation Environment for Cyber Attack Analysis and Response in Thailand

อนุรักษ์ ตันตราธิปไตย

นักศึกษาระดับปริญญาเอก

บทคัดย่อ

โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศมีบทบาทสำคัญอย่างยิ่งต่อการดำเนินงานของทั้งภาครัฐและภาคเอกชน อย่างไรก็ตาม ภัยคุกคามทางไซเบอร์มีแนวโน้มเพิ่มขึ้นทั้งในด้านความถี่และความซับซ้อน เช่น Malware, Phishing, Distributed Denial of Service (DDoS) และการโจมตีแบบ Zero Day ซึ่งระบบความมั่นคงปลอดภัยแบบดั้งเดิมที่อาศัยกฎหรือรูปแบบคงที่ไม่สามารถตรวจจับและตอบสนองได้อย่างมีประสิทธิภาพในสภาพแวดล้อมที่เปลี่ยนแปลงอย่างรวดเร็ว อีกทั้งการทดสอบมาตรการด้านความปลอดภัยในระบบจริงยังมีความเสี่ยงต่อการหยุดชะงักของบริการและความเสียหายต่อองค์กร งานวิจัยนี้มีวัตถุประสงค์เพื่อพัฒนา สภาพแวดล้อมจำลองอัจฉริยะสำหรับการวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ในประเทศไทย โดยประยุกต์ใช้แนวคิดของทฤษฎีระบบจำลองร่วมกับเทคโนโลยีปัญญาประดิษฐ์ (AI/ML) เพื่อสร้างแพลตฟอร์มที่สามารถจำลองโครงสร้างพื้นฐานไอทีที่ใกล้เคียงกับระบบจริง จำลองสถานการณ์การโจมตีทางไซเบอร์หลากหลายรูปแบบ และสนับสนุนการตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามแบบอัตโนมัติ นอกจากนี้ระบบยังออกแบบให้สามารถประเมินความสอดคล้องกับกรอบมาตรฐานความมั่นคงปลอดภัยไซเบอร์สากล เช่น NIST Cybersecurity Framework และ ISO/IEC 27001 วิธีดำเนินการวิจัยประกอบด้วยการออกแบบสภาพแวดล้อมจำลองแบบเสมือน การสร้างสถานการณ์โจมตีเชิงทดลอง การฝึกและทดสอบโมเดล AI/ML สำหรับการตรวจจับและตอบสนอง รวมถึงการประเมินผลด้วยตัวชี้วัดด้านความแม่นยำในการตรวจจับ เวลาตอบสนอง และระดับการปฏิบัติตามมาตรฐาน ผลการวิจัยแสดงให้เห็นว่าระบบจำลองอัจฉริยะสามารถช่วยลดระยะเวลาในการตอบสนอง เพิ่มประสิทธิภาพในการวิเคราะห์ภัยคุกคาม และสนับสนุนการยกระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กรในประเทศไทยได้อย่างมีประสิทธิภาพ

คำสำคัญ : Preemptive Cybersecurity , Intelligent Environment , Cybersecurity Simulation , AI-based Threat Analysis and Response

1. บทนำ

ในยุคดิจิทัล โครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ ได้กลายเป็นกลไกสำคัญของการดำเนินงานทั้งภาครัฐและเอกชน แต่ขณะเดียวกันภูมิทัศน์ภัยคุกคามไซเบอร์กลับทวีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว ตั้งแต่มัลแวร์ การโจมตีแบบฟิชชิง การโจมตีแบบ DDoS ไปจนถึง Zero day และ APT ที่ซ่อนตัวเนิ่นนาน ทำให้กลไกป้องกันแบบเดิมมีข้อจำกัดทั้งด้านความแม่นยำและความทันเวลาในการตอบสนอง [1] [2] แนวโน้มดังกล่าวสะท้อนชัด จากงานทบทวนเชิงระบบที่ชี้ว่าแนวทาง AI/ML และ DL ซึ่งประมวลรูปแบบข้อมูลขนาดใหญ่และซับซ้อน สามารถยกระดับการตรวจจับและลดเวลาการตอบสนองได้เหนือกว่าวิธีดั้งเดิม แต่ก็ยังต้องออกแบบให้สอดรับกับภัยสมัยใหม่และลด Data Bias [1][3]

หนึ่งในช่องว่างสำคัญของงานประยุกต์คือ การขาดสภาพแวดล้อมที่สมจริงและปลอดภัยสำหรับทดสอบป้องกัน ตรวจจับ ตอบสนอง โดยไม่กระทบระบบจริง งานทบทวนล่าสุดระบุว่าชุดเครื่องมือจำลองการโจมตียังขาดความครอบคลุมเชิงสถานการณ์และความสามารถบูรณาการ AI powered attacks/defenses แบบครบวงจร ทำให้ผลการประเมินอาจมีความไม่ถูกต้องและยากต่อการเทียบเคียง [4][5] ทั้งนี้ทฤษฎีระบบจำลองช่วยให้นักวิจัยควบคุมตัวแปร ทดลองซ้ำ และวิเคราะห์พฤติกรรมระบบภายใต้เงื่อนไขที่กำหนดได้อย่างปลอดภัย จึงเหมาะสำหรับศึกษาปฏิสัมพันธ์เชิงซับซ้อนของโครงสร้างพื้นฐานไอทีและภัยคุกคาม [4] [6]

พร้อมกันนั้นกรอบมาตรฐานความมั่นคงปลอดภัยสากล เช่น NIST Cybersecurity Framework และ ISO/IEC 27001 ได้รับการยอมรับอย่างกว้างขวางในการจัดการความเสี่ยงและยกระดับความพร้อมขององค์กร หากสามารถเชื่อมโยงผลการจำลองเข้ากับข้อกำหนดและการคอนโทรลของกรอบดังกล่าว จะช่วยให้การประเมินมีความหมายเชิงปฏิบัติการและตรวจสอบได้ [7][8] งานบูรณาการกรอบมาตรฐานกับเทคโนโลยี AI/ML ยังย้ำว่าการกำกับดูแล ความโปร่งใส และตัวชี้วัดประสิทธิผลเป็นปัจจัยจำเป็นต่อการประยุกต์ใช้จริง [7] ขณะเดียวกันความท้าทายเชิงเทคนิคใหม่ ๆ เช่น Adversarial ML ก็ผลักดันให้การออกแบบระบบตรวจจับและตอบสนองต้องคำนึงถึงยุทธวิธีหลบเลี่ยงโมเดล และการคงความน่าเชื่อถือของ AI ตลอดวัฏจักรการโจมตี [9]
จากภูมิหลังดังกล่าวปัญหาวิจัยหลัก คือ การขาดแพลตฟอร์มสภาพแวดล้อมจำลองอัจฉริยะ ที่ผสานการจำลองโครงสร้างพื้นฐานไอทีให้ใกล้เคียงระบบจริง การจำลองการโจมตีหลายรูปแบบ การตรวจจับวิเคราะห์ด้วย AI/ML และการตอบสนองอัตโนมัติ และการประเมินความสอดคล้องตามมาตรฐาน NIST/ISO 27001 ภายใต้ตัวชี้วัดเชิงหลักฐานเดียวกัน หากไม่ ทำวิจัยพัฒนาแพลตฟอร์มดังกล่าว องค์กรจะยังต้องทดสอบบนระบบจริงที่มีความเสี่ยงสูง ไม่สามารถเรียนรู้ปรับตัวได้เชิงรุก และไม่อาจพิสูจน์ความสอดคล้องตามมาตรฐานด้วยข้อมูลทดลองที่ทำซ้ำและตรวจสอบได้ ส่งผลให้เวลาตรวจจับและตอบสนองยืดเยื้อใช้เวลายาวนาน ความเสียหายทวีคูณ และความเชื่อมั่นเชิงนโยบายและกำกับดูแลถดถอย [1][8]

ดังนั้นงานวิจัยนี้จึงมุ่งพัฒนา สภาพแวดล้อมจำลองอัจฉริยะสำหรับการวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ในประเทศไทย โดยใช้ Simulation based Design ผสาน AI/ML เพื่อการ

ตรวจจับและตอบสนองเชิงรุก และผูกผลลัพธ์กับกรอบ NIST/ISO 27001 อย่างเป็นระบบ พร้อมยืนยันผลด้วยตัวชี้วัดด้านความแม่นยำ เวลาตอบสนอง อัตราความผิดพลาด และระดับการปฏิบัติตามมาตรฐาน เพื่อยกระดับ Cybersecurity Resilience ขององค์กรไทย [1][7] [4][8]

2. วัตถุประสงค์

2.1 วัตถุประสงค์หลักของการวิจัย

การวิจัยนี้มีวัตถุประสงค์หลักเพื่อพัฒนาและประเมินสภาพแวดล้อมจำลองอัจฉริยะสำหรับการวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ในประเทศไทย โดยมีจุดมุ่งหมายเพื่อค้นหาคำตอบตามปัญหาวิจัย ดังต่อไปนี้

2.1.1 เพื่อช่วยลดเวลาความเสียหายและรองรับการกู้คืนระบบได้รวดเร็วขึ้น ในการถูกภัยคุกคามไซเบอร์โจมตี แบบจำลองนี้จะเป็นต้นแบบเพื่อนำไปประยุต์ใช้จริง ช่วยผู้ดูแลระบบตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนและเปลี่ยนแปลงได้อย่างรวดเร็ว

2.1.2 เพื่อออกแบบและพัฒนาสภาพแวดล้อมจำลองโครงสร้างพื้นฐานไอที ที่มีความใกล้เคียงกับระบบจริง พร้อมทั้งมีความปลอดภัยและสามารถควบคุมการทดลองได้โดยไม่กระทบต่อระบบจริงขององค์กร

2.1.3 เพื่อจำลองและวิเคราะห์สถานการณ์การโจมตีทางไซเบอร์หลายรูปแบบ เช่น Malware, Phishing, DDoS และ Zero day attack เพื่อประเมินประสิทธิภาพของการตรวจจับและการตอบสนองของระบบ

2.1.4 เพื่อพัฒนาและประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง AI/ML ในการตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามทางไซเบอร์แบบอัตโนมัติ

2.1.5 เพื่อประเมินประสิทธิภาพของสภาพแวดล้อมจำลองอัจฉริยะที่พัฒนาขึ้น โดยใช้ตัวชี้วัดด้านความแม่นยำในการตรวจจับ เวลาตอบสนอง และอัตราความผิดพลาดของระบบ

2.2 วัตถุประสงค์รองของการวิจัย

นอกจากวัตถุประสงค์หลักแล้ว การวิจัยนี้ยังมีวัตถุประสงค์รองเพื่อสนับสนุนการนำไปใช้งานและการต่อยอดองค์ความรู้ ดังนี้

2.2.1 เพื่อประเมินความสอดคล้องของระบบกับกรอบมาตรฐานความมั่นคงปลอดภัยไซเบอร์สากล เช่น NIST Cybersecurity Framework และ ISO/IEC 27001

2.2.2 เพื่อสนับสนุนการฝึกอบรมและพัฒนาศักยภาพบุคลากรด้านความมั่นคงปลอดภัยไซ

เบอร์ ผ่านการใช้สภาพแวดล้อมจำลองที่ใกล้เคียงกับสถานการณ์จริง

2.2.3 เพื่อเสนอแนวทางในการพัฒนาระบบความมั่นคงปลอดภัยไซเบอร์เชิงรุก ที่สามารถเรียนรู้และปรับตัวจากผลการทดลองในสภาพแวดล้อมจำลอง

2.2.4 เพื่อสร้างต้นแบบเชิงแนวคิดที่สามารถนำไปต่อยอดใช้ในองค์กรภาครัฐและภาคเอกชนในประเทศไทย รวมถึงการพัฒนาเชิงนโยบายหรือเชิงพาณิชย์ในอนาคต

3. ขอบเขตของการวิจัย

งานวิจัยนี้เป็นการวิจัยเชิงพัฒนาและเชิงทดลอง มีขอบเขตการศึกษาเพื่อให้การดำเนินงานเป็นไปอย่างชัดเจนและสามารถประเมินผลได้อย่างเป็นระบบ ดังรายละเอียดต่อไปนี้

3.1 ประชากร

ประชากรของการวิจัย ได้แก่ สภาพแวดล้อมโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและระบบความมั่นคงปลอดภัยไซเบอร์ขององค์กรในประเทศไทย ทั้งในภาครัฐและภาคเอกชน ซึ่งมีลักษณะการใช้งานโครงสร้างพื้นฐานไอทีประกอบด้วยระบบเครือข่าย เซิร์ฟเวอร์ ระบบฐานข้อมูล และระบบรักษาความปลอดภัย เช่น Firewall, IDS/IPS และ SIEM ประชากรดังกล่าวครอบคลุมบริบทขององค์กรที่มีความเสี่ยงต่อภัยคุกคามทางไซเบอร์รูปแบบต่าง ๆ อาทิ Malware, Phishing, DDoS และ Advanced Persistent Threats (APTs) ตามที่ได้รับการรายงานในงานวิจัยและรายงานความมั่นคงปลอดภัยไซเบอร์ระดับสากล [1][2]

3.2 กลุ่มตัวอย่าง

กลุ่มตัวอย่างของการวิจัย ได้แก่ สภาพแวดล้อมจำลองโครงสร้างพื้นฐานไอที ที่ผู้วิจัยออกแบบและพัฒนาขึ้น โดยอ้างอิงสถาปัตยกรรมโครงสร้างพื้นฐานขององค์กรทั่วไปในประเทศไทย และใช้เป็นสนามทดลอง สำหรับการจำลองการโจมตีและการตอบสนองต่อภัยคุกคามทางไซเบอร์ การเลือกกลุ่มตัวอย่างเป็นการเลือกแบบเจาะจง เพื่อให้สอดคล้องกับวัตถุประสงค์ของการวิจัย และเป็นแนวทางที่นิยมใช้ในการวิจัยด้านระบบจำลองและความมั่นคงปลอดภัยไซเบอร์ [4][10]

3.3 ตัวแปรในการวิจัย

การวิจัยครั้งนี้กำหนดตัวแปรที่ใช้ศึกษาออกเป็น 2 ประเภท ดังนี้

3.3.1 ตัวแปรอิสระ

ตัวแปรอิสระ ได้แก่

1. รูปแบบของภัยคุกคามทางไซเบอร์ที่ถูกจำลอง Malware เช่น Malware , Phishing , Distributed Denial of Service (DDoS) , Zero day attack เป็นต้น
2. เทคนิคและโมเดลด้าน AI/ML ที่ใช้ในการวิเคราะห์และตรวจจับภัยคุกคาม เช่น Supervised Learning , Unsupervised Learning , Deep Learning เป็นต้น
3. กลไกการตอบสนองอัตโนมัติของระบบ เช่น การแจ้งเตือน การบล็อก และการกักกันระบบ

3.3.2 ตัวแปรตาม

ตัวแปรตาม ได้แก่

1. ความแม่นยำในการตรวจจับภัยคุกคาม
2. ระยะเวลาในการตอบสนองต่อเหตุการณ์
3. อัตราความผิดพลาดของระบบ
4. ระดับความสอดคล้องกับมาตรฐานความมั่นคงปลอดภัยไซเบอร์สากล เช่น NIST และ ISO/IEC 27001

ตัวแปรตามเหล่านี้เป็นตัวชี้วัดที่ได้รับการนำมาใช้ประเมินประสิทธิภาพของระบบตรวจจับและตอบสนองต่อภัยคุกคามในงานวิจัยด้าน Cybersecurity อย่างแพร่หลาย [1][11]

3.4 ระยะเวลาในการวิจัย

การวิจัยครั้งนี้ดำเนินการภายในระยะเวลา 12 เดือน โดยแบ่งช่วงการดำเนินงานออกเป็น 4 ระยะ ได้แก่

1. การศึกษางานวิจัยและเอกสารที่เกี่ยวข้อง เดือนที่ 1 ถึงเดือนที่ 3
2. การออกแบบและพัฒนาสภาพแวดล้อมจำลองอัจฉริยะ เดือนที่ 4 ถึงเดือนที่ 6
3. การทดลอง จำลองสถานการณ์โจมตี และเก็บรวบรวมข้อมูล เดือนที่ 7 ถึงเดือนที่ 9
4. การวิเคราะห์ข้อมูล สรุปผล และจัดทำรายงานวิจัย เดือนที่ 10 ถึงเดือนที่ 12

4. ประโยชน์ที่คาดว่าจะได้รับ

การพัฒนางานวิจัยเรื่อง การจำลองสภาพแวดล้อมอัจฉริยะสำหรับการวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ในประเทศไทย คาดว่าจะก่อให้เกิดประโยชน์ทั้งในเชิงวิชาการ เชิงปฏิบัติ และเชิงนโยบาย ดังรายละเอียดต่อไปนี้

4.1 ประโยชน์เชิงวิชาการและการเพิ่มพูนองค์ความรู้

ประโยชน์ที่สำคัญประการแรกของงานวิจัยนี้ คือ การเพิ่มพูนองค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ในเชิงระบบจำลองอัจฉริยะ โดยงานวิจัยได้บูรณาการแนวคิดของทฤษฎีระบบจำลอง เข้ากับเทคโนโลยีปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง AI/ML เพื่อศึกษาพฤติกรรมของโครงสร้างพื้นฐานไอทีและภัยคุกคามทางไซเบอร์ในสภาพแวดล้อมที่ควบคุมได้ การประยุกต์ใช้สภาพแวดล้อมจำลองช่วยให้นักวิจัยสามารถทดลองซ้ำ วิเคราะห์ผลกระทบ และเปรียบเทียบแนวทางการตรวจจับและตอบสนองต่อภัยคุกคามได้อย่างเป็นระบบ ซึ่งสอดคล้องกับงานวิจัยก่อนหน้าที่ชี้ว่าการใช้ Cyber Range และ Attack Simulation เป็นเครื่องมือสำคัญในการศึกษาปฏิสัมพันธ์เชิงซับซ้อนของระบบความมั่นคงปลอดภัยไซเบอร์ [1][4] นอกจากนี้งานวิจัยยังช่วยขยายองค์ความรู้ด้าน Preemptive Cybersecurity ซึ่งเป็นแนวคิดการป้องกันเชิงรุก โดยใช้ AI/ML เพื่อคาดการณ์ วิเคราะห์ และตอบสนองต่อภัยคุกคามก่อนที่จะเกิดความเสียหายรุนแรงต่อระบบจริง แนวคิดดังกล่าวได้รับการกล่าวถึงอย่างกว้างขวางในวรรณกรรมด้าน Cybersecurity สมัยใหม่ แต่ยังขาดการศึกษาผ่านแพลตฟอร์มจำลองที่สมจริงและสามารถเชื่อมโยงกับการปฏิบัติตามมาตรฐานได้อย่างเป็นรูปธรรม [12][3]

4.2 ประโยชน์เชิงปฏิบัติ การประยุกต์ใช้ และการพัฒนาคุณภาพ

ในเชิงปฏิบัติ งานวิจัยนี้คาดว่าจะเป็น แนวทางต้นแบบ Prototype Framework สำหรับองค์กรในประเทศไทยในการนำไปใช้ทดสอบระบบความมั่นคงปลอดภัยไซเบอร์โดยไม่กระทบต่อระบบผลิตจริง ช่วยลดความเสี่ยงจากการทดสอบในสภาพแวดล้อมจริง ซึ่งเป็นข้อจำกัดสำคัญขององค์กรจำนวนมาก [4][11] สภาพแวดล้อมจำลองอัจฉริยะที่พัฒนาขึ้นสามารถนำไปใช้เป็นเครื่องมือฝึกอบรมบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ผ่านสถานการณ์โจมตีที่ใกล้เคียงกับเหตุการณ์จริง ส่งผลให้บุคลากรมีความพร้อมในการตรวจจับ วิเคราะห์ และตอบสนองต่อเหตุการณ์ได้อย่างมีประสิทธิภาพ ซึ่งสอดคล้องกับแนวทางการพัฒนา Cybersecurity Resilience ที่เสนอให้ใช้การฝึกซ้อมผ่าน Cyber Range เป็นกลไกหลัก [1][10] ยิ่งไปกว่านั้นงานวิจัยยังมี

ประโยชน์ในด้าน การประเมินความสอดคล้องกับกรอบมาตรฐานความมั่นคงปลอดภัยสากล เช่น NIST Cybersecurity Framework และ ISO/IEC 27001 โดยเชื่อมโยงผลการทดลองในสภาพแวดล้อมจำลองเข้ากับตัวชี้วัดด้านการปฏิบัติตามมาตรฐานอย่างเป็นระบบ ซึ่งช่วยให้องค์กรสามารถใช้ผลการวิจัยเป็นข้อมูลประกอบการตรวจประเมิน การปรับปรุงนโยบาย และการตัดสินใจเชิงบริหารได้อย่างมีหลักฐานรองรับ [11][8] ในภาพรวมงานวิจัยนี้มีศักยภาพในการยกระดับคุณภาพของระบบความมั่นคงปลอดภัยไซเบอร์ขององค์กรไทย สนับสนุนการพัฒนานโยบายด้านความมั่นคงปลอดภัยสารสนเทศ และสามารถต่อยอดไปสู่การพัฒนาแพลตฟอร์มเชิงพาณิชย์หรือการใช้งานในระดับประเทศในอนาคต

5. กรอบแนวคิดการวิจัย

การวิจัยเรื่องการจำลองสภาพแวดล้อมอัจฉริยะสำหรับการวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ในประเทศไทย" ได้รับการออกแบบบนฐานของทฤษฎีและแนวคิดหลักสี่ประการ ได้แก่ ทฤษฎีระบบจำลอง ทฤษฎีการเรียนรู้ของเครื่อง ทฤษฎีการตอบสนองต่อเหตุการณ์ กรอบมาตรฐานความมั่นคงปลอดภัยไซเบอร์ ซึ่งแต่ละแนวคิดช่วยกำหนดความสัมพันธ์ระหว่างตัวแปรและกระบวนการต่าง ๆ ในการพัฒนาสภาพแวดล้อมจำลองอัจฉริยะ ที่ใช้ตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

5.1 ทฤษฎีพื้นฐานที่เกี่ยวข้อง

5.1.1 ทฤษฎีระบบจำลอง

ทฤษฎีระบบจำลองอธิบายการสร้างแบบจำลองของระบบจริงเพื่อศึกษาพฤติกรรมภายใต้สภาวะและปัจจัยต่าง ๆ โดยมีข้อได้เปรียบในการควบคุมตัวแปร ทดลองซ้ำ และลดความเสี่ยงจากการทดสอบบนระบบจริง การประยุกต์ Simulation ถูกเสนอว่าเป็นแนวทางสำคัญในการทดสอบระบบความมั่นคงปลอดภัยไซเบอร์อย่างปลอดภัยและสมจริง โดยเฉพาะ Cyber Attack Modeling และ Cyber Range Tools ตามงานวิจัยของ Jaber & Fritsch (2023) ซึ่งชี้ว่าการใช้ Simulation เป็นรากฐานสำหรับการสร้างสภาพแวดล้อมการทดสอบภัยคุกคามไซเบอร์ที่มีความแม่นยำเชิงสถานการณ์ [13]

5.1.2 ทฤษฎีการเรียนรู้ของเครื่อง

Machine Learning และ Deep Learning เป็นกลไกสำคัญในการประมวลผลข้อมูลภัยคุกคามขนาดใหญ่และการตรวจจับพฤติกรรมผิดปกติแบบอัตโนมัติ โดยงานของ Salem et al. (2024)

ระบุว่า AI/ML สามารถเพิ่มความแม่นยำในการตรวจจับภัยคุกคามได้อย่างมีนัยสำคัญเหนือ signature-based systems และช่วยลดเวลาตอบสนอง ได้อย่างเด่นชัด [14] นอกจากนี้ Kutagamari (2025) ยังชี้ให้เห็นถึงความจำเป็นของการออกแบบโมเดล ML ให้รองรับภัยยุคใหม่และลดอคติของข้อมูล (Model Bias) เพื่อให้ระบบตรวจจับทำงานได้อย่างมีเสถียรภาพในสถานการณ์จริง [15]

5.1.3 ทฤษฎีการตอบสนองต่อเหตุการณ์

ตามแนวคิด Incident Response ของ NIST (SP 800-61) ขั้นตอนการจัดการเหตุการณ์ต้องประกอบด้วยการตรวจจับ วิเคราะห์ ควบคุม กำจัด และฟื้นฟู โดยต้องอาศัย Automation เพื่อเพิ่มความรวดเร็วตามมาตรฐาน NIST CSF และงานของ Essien et al. (2024) ที่เสนอโมเดลตอบสนองต่อเหตุการณ์โดยผสาน ISO 27001 และ NIST เพื่อเพิ่มประสิทธิภาพการตอบสนองและลดระยะเวลาความเสียหาย [16]

5.1.4 กรอบมาตรฐานความมั่นคงปลอดภัยไซเบอร์

มาตรฐานสากลอย่าง NIST CSF และ ISO/IEC 27001 เป็นแนวทางหลักที่องค์กรใช้ประเมินระดับความมั่นคงปลอดภัยและความพร้อมในการรับมือเหตุการณ์ไซเบอร์ งานของ Lokare et al. (2025) ชี้ว่าองค์กรจำเป็นต้องประเมินระบบตามกรอบมาตรฐานดังกล่าวเพื่อให้การป้องกันภัยไซเบอร์มีความน่าเชื่อถือและตรวจสอบได้[17]

5.2 ตัวแปรและความสัมพันธ์ระหว่างตัวแปร

จากทฤษฎีและงานวิจัยข้างต้น สามารถกำหนดความสัมพันธ์ของตัวแปรในงานวิจัยได้ดังนี้

5.2.1 ตัวแปรอิสระ

ประเภทของภัยคุกคามที่ถูกจำลอง (Malware, Phishing, DDoS, Zero Day) [18] เทคนิคและโมเดล AI/ML ที่ใช้ในการวิเคราะห์และตรวจจับภัยคุกคาม (Random Forest, LSTM, Autoencoder ฯลฯ) [14]

กลไกการตอบสนองอัตโนมัติของระบบ (SOAR, Automated Response Policies) [16]

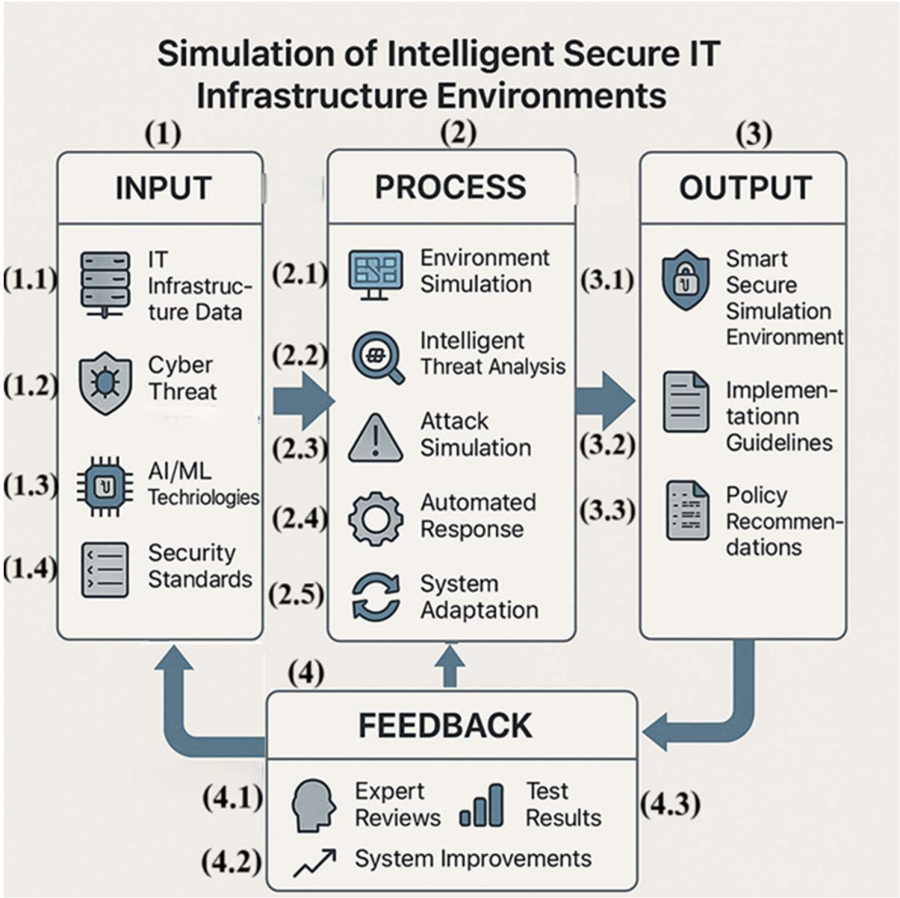
5.2.2 ตัวแปรตาม

ความแม่นยำในการตรวจจับภัยคุกคาม (Detection Accuracy) เวลาตอบสนองต่อเหตุการณ์ (Response Time) อัตราการแจ้งเตือนผิดพลาด (False Positive/Negative Rate) ระดับความสอดคล้องตามมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Compliance Level)

ตัวแปรเหล่านี้ตรงกับตัวชี้วัดที่ใช้ในงานประเมินระบบ Cybersecurity Simulation และ AI-based Threat Detection ในงานวิจัยระดับนานาชาติ เช่น Mallick & Nath (2024) [18]

5.3 กรอบแนวคิดสำหรับการพัฒนางานวิจัย

จากการสังเคราะห์องค์ความรู้ด้าน Simulation, AI/ML, Incident Response และ Cybersecurity Standards สามารถสร้างกรอบแนวคิดการวิจัย สำหรับการพัฒนาสภาพแวดล้อมจำลองอัจฉริยะเพื่อการวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ดังภาพที่ 1



ภาพที่ 1 กรอบแนวคิดการวิจัยการพัฒนาสภาพแวดล้อมจำลองอัจฉริยะเพื่อการวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ในประเทศไทย

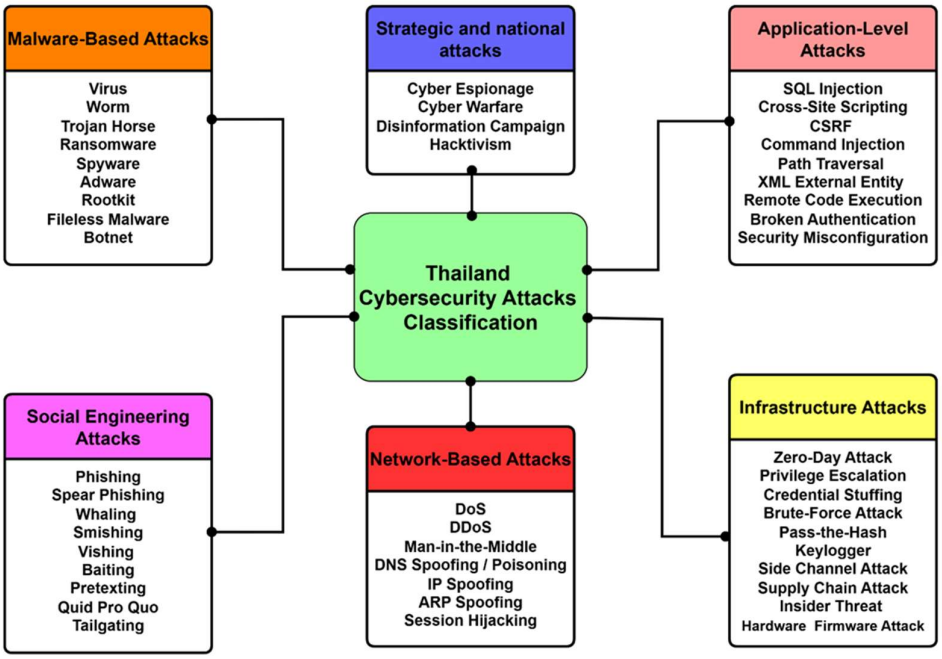
ภาพที่ 1 แสดงกรอบแนวคิดการวิจัยสำหรับการพัฒนาสภาพแวดล้อมจำลองอัจฉริยะเพื่อการวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ โดยประกอบด้วย 4 องค์ประกอบหลัก ได้แก่

INPUT , PROCESS , OUTPUT , FEEDBACK ซึ่งทำงานสัมพันธ์กันเป็นวงจรต่อเนื่อง เพื่อยกระดับความมั่นคงปลอดภัยของโครงสร้างพื้นฐานไอที

(1) INPUT ส่วนนี้คือข้อมูลและองค์ประกอบต้นทาง ที่จำเป็นต่อการสร้างสภาพแวดล้อมจำลองอัจฉริยะ ประกอบด้วย

(1.1) IT Infrastructure Data เป็นข้อมูลโครงสร้างพื้นฐานไอที เช่น Network topology, Server roles, Security devices ซึ่งใช้เพื่อสร้างแบบจำลองระบบที่เสมือนจริงมากที่สุด โดยข้อมูลนี้จะช่วยให้การจำลองมีความแม่นยำและสะท้อนสภาวะจริงขององค์กร

(1.2) Cyber Threat Intelligence เป็นข้อมูลภัยคุกคาม เช่น Indicator of Compromise (IOC), Tactics Techniques and Procedures (TTPs) และรูปแบบโจมตี Malware, Phishing, DDoS) รวมถึงข้อมูลการจัดกลุ่มภัยคุกคามที่ได้จากการดำเนินการสนทนากลุ่ม (Focus Group) ร่วมกับผู้เชี่ยวชาญที่มีประสบการณ์ด้านโครงสร้างพื้นฐานและความมั่นคงปลอดภัยไซเบอร์ในระดับองค์กรและระดับประเทศ โดยข้อมูลนี้จะใช้สำหรับสร้างสถานการณ์การโจมตีในระบบจำลอง



ภาพที่ 2 Thailand Cybersecurity Attacks Classification

ภาพที่2 จากการดำเนินการสนทนากลุ่ม (Focus Group) ร่วมกับผู้เชี่ยวชาญที่มีประสบการณ์ด้านโครงสร้างพื้นฐานและความมั่นคงปลอดภัยไซเบอร์ในระดับองค์กรและระดับประเทศ ผู้วิจัยได้รวบรวมและวิเคราะห์ภัยคุกคามทางไซเบอร์จำนวนทั้งสิ้น 48 รายการ โดยอ้างอิงจากแหล่งข้อมูลที่เชื่อถือได้ เช่น รายงานจากหน่วยงานด้านความมั่นคงไซเบอร์ทั้งในประเทศและต่างประเทศ รวมถึงเหตุการณ์ที่เกิดขึ้นจริงในบริบทของประเทศไทย [19][20] ผลการวิเคราะห์นำไปสู่การพัฒนาแนวทางการจำแนกกลุ่มภัยคุกคามออกเป็น 6 หมวดหลัก ได้แก่

1.การโจมตีโดยอาศัยมัลแวร์ (Malware-Based Attacks)

2.การโจมตีทางเครือข่าย (Network-Based Attacks)

3.การโจมตีระดับแอปพลิเคชัน (Application-Level Attacks)

4.การโจมตีด้วยเทคนิคทางสังคม (Social Engineering Attacks)

5.การโจมตีโครงสร้างพื้นฐาน (Infrastructure Attacks)

6.การโจมตีเชิงยุทธศาสตร์ระดับประเทศ (Strategic/Nation-State Attacks)

การจำแนกดังกล่าวเป็นองค์ประกอบสำคัญของกรอบแนวคิด Thailand Cybersecurity Attacks Classification Framework ที่นำเสนอในงานวิจัยฉบับนี้ โดยมีเป้าหมายเพื่อใช้เป็นเครื่องมือในการวิเคราะห์ภัยคุกคาม การประเมินความเสี่ยง และการกำหนดนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ในระดับองค์กรและระดับประเทศอย่างเป็นระบบ [21]

(1.3) AI/ML Technologies เป็นโมเดล Machine Learning / Deep Learning ที่ใช้ตรวจจับและวิเคราะห์ภัย เช่น Random Forest, LSTM, Autoencoder โดยทำหน้าที่เป็นสมองอัจฉริยะของระบบ

(1.4) Security Standards กรอบมาตรฐานความมั่นคงปลอดภัย เช่น NIST CSF, ISO/IEC 27001 โดยจะเป็นเกณฑ์ในการประเมินความพร้อมด้านความมั่นคงปลอดภัยขององค์กร

(2) PROCESS ส่วนนี้คือหัวใจของการวิจัย เป็นกลไกการทำงานภายในระบบจำลองประกอบด้วย 5 โมดูลหลัก

(2.1) Environment Simulation เป็นการสร้างสภาพแวดล้อมโครงสร้างพื้นฐานไอทีเสมือนที่ใกล้เคียงของจริง เช่น Virtual network, Virtual servers เพื่อให้ก่อเกิดบริบทที่เหมาะสมต่อการทดลอง

(2.2) Intelligent Threat Analysis เป็นการวิเคราะห์ภัยคุกคามด้วย AI/ML โดยนำข้อมูลจาก Cyber Threat Intelligence มาประมวลผล โดยจะช่วยตรวจจับพฤติกรรมผิดปกติได้แบบอัตโนมัติและทันสมัยกว่า signature-based

(2.3) Attack Simulation เป็นการจำลองสถานการณ์การโจมตี เช่น Malware infection, DDoS flooding, Unauthorized access โดยใช้ทดสอบระบบป้องกันและระบบวิเคราะห์ภัย

(2.4) Automated Response เป็นกลไกตอบสนองภัยอัตโนมัติ เช่น Block traffic, Quarantine node, Alert to admin โดยจะช่วยลดเวลา MTTR (Mean Time to Response) อย่างมีนัยสำคัญ

(2.5) System Adaptation เป็นการเรียนรู้และปรับปรุงระบบอัตโนมัติจากผลการทดสอบ เช่น Model retraining, Policy fine-tuning โดยช่วยทำให้ระบบฉลาดขึ้น ทุกครั้งที่มีการโจมตีใหม่

(3) OUTPUT ส่วนนี้คือสิ่งที่ได้จากการใช้สภาพแวดล้อมจำลองอัจฉริยะ โดยรวมผลลัพธ์ทั้งด้านเทคนิคและด้านนโยบาย

(3.1) Smart Secure Simulation Environment เป็นระบบจำลองอัจฉริยะที่พร้อมใช้งานสำหรับองค์กร เพื่อทดสอบ วิเคราะห์ และเตรียมความพร้อมด้านความปลอดภัย

(3.2) Implementation Guidelines เป็นแนวทางการนำไปใช้งานในองค์กร เช่น ขั้นตอนการตั้งค่า ข้อควรระวัง และนโยบายการใช้งาน

(3.3) Policy Recommendations เป็นข้อเสนอเชิงนโยบาย เช่น การกำหนดมาตรฐาน การจัดสรรทรัพยากรด้าน Cybersecurity และแผนอบรมบุคลากร

(4) FEEDBACK เป็นองค์ประกอบสำคัญที่ทำให้ระบบพัฒนาอย่างต่อเนื่อง

(4.1) Expert Reviews ผู้เชี่ยวชาญด้าน Cybersecurity ตรวจสอบความถูกต้อง ความสมจริง และความครบถ้วน

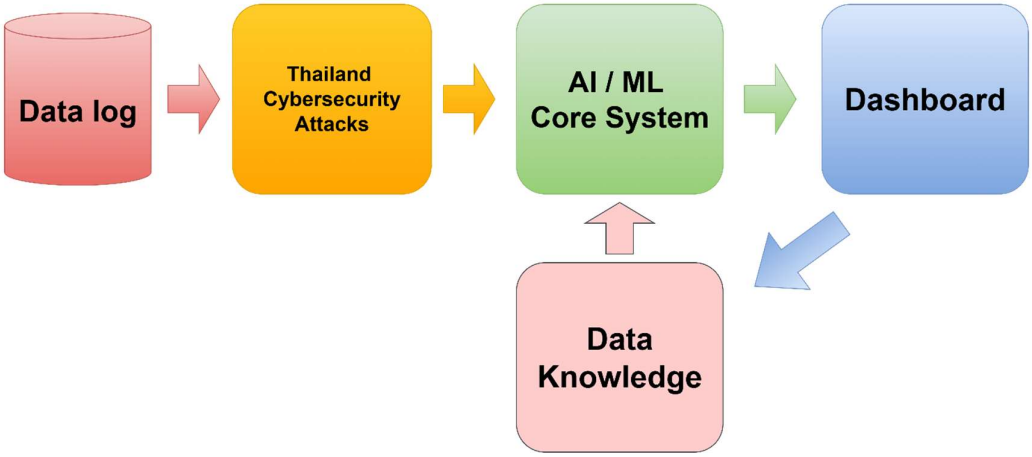
(4.2) Test Results ผลการจำลอง เช่น Accuracy, Response Time, Attack detection rate ใช้วิเคราะห์และหาจุดที่ต้องปรับปรุง

(4.3) System Improvements การนำข้อมูลจาก (4.1) และ (4.2) กลับไปปรับปรุงส่วน INPUT และ PROCESS ทำให้ระบบพัฒนาอย่างต่อเนื่องและแข็งแกร่งขึ้นทุกการทดลอง

ภาพที่1 แสดงให้เห็นว่าการพัฒนาสภาพแวดล้อมจำลองอัจฉริยะต้องพึ่งพา ข้อมูลโครงสร้างพื้นฐาน ภัยคุกคาม เทคโนโลยี AI/ML และ มาตรฐานความปลอดภัย
ระบบจำลองประกอบด้วยกระบวนการ 5 ขั้นตอน ตั้งแต่การจำลองสภาพแวดล้อมไปจนถึงการตอบสนองอัตโนมัติ ผลลัพธ์ที่ได้ตอบโจทย์ทั้งระดับเทคนิค และระดับองค์กร/นโยบาย

มีการทำงานแบบวนซ้ำ เพื่อให้ระบบเรียนรู้ ปรับตัว พัฒนาอย่างต่อเนื่อง นี่คือโมเดลที่สมบูรณ์สำหรับงานวิจัยด้าน Cybersecurity ที่เน้นการจำลอง การวิเคราะห์ และการตอบสนองต่อภัยคุกคามด้วย AI/ML

งานวิจัยจำนวนมากได้แสดงให้เห็นว่า AI และ ML มีบทบาทสำคัญในการเสริมสร้างความสามารถในการตรวจจับและตอบสนองต่อภัยคุกคามแบบเรียลไทม์ [22] เทคนิคที่นิยมใช้ได้แก่ Supervised Learning, Unsupervised Learning, Reinforcement Learning และ Deep Learning ซึ่งสามารถนำไปใช้ในระบบ SIEM, Threat Intelligence Platforms และระบบตอบสนองอัตโนมัติ [23] [24]



ภาพที่ 3 A Conceptual Framework for an Intelligent System for Cyber Attack Analysis and Response in Thailand

ภาพที่ 3 แสดงกรอบแนวคิดของระบบอัจฉริยะที่ออกแบบมาเพื่อวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ในบริบทของประเทศไทย โดยประกอบด้วยองค์ประกอบหลัก 5 ส่วนที่เชื่อมโยงกันผ่านกระบวนการไหลของข้อมูล ได้แก่

1. Data Log เป็นแหล่งรวบรวมข้อมูลเหตุการณ์ทางไซเบอร์จากระบบต่าง ๆ เช่น Firewall, IDS/IPS และ ระบบเครือข่าย โดยข้อมูลเหล่านี้จะถูกนำไปใช้ในการวิเคราะห์เบื้องต้น [25]
2. Thailand Cybersecurity Attacks เป็นฐานข้อมูลที่จำแนกประเภท 48 ภัยคุกคามที่

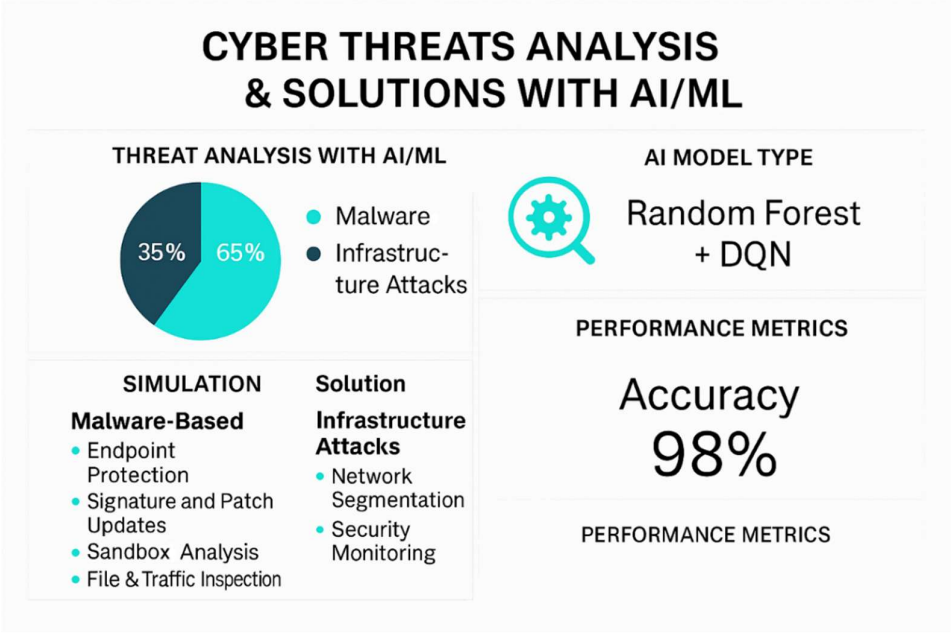
เกิดขึ้นจริงในประเทศไทย หมวดหมู่หลัก 6 ประเภท ได้แก่ Malware-Based, Network-Based, Application-Level, Social Engineering, Infrastructure และ Strategic/Nation-State Attacks โดยอิงจากการสนทนากลุ่ม (Focus Group)

3. AI / ML Core System เป็นแกนกลางของระบบที่ใช้เทคโนโลยีปัญญาประดิษฐ์และการเรียนรู้ของเครื่องใน การตรวจจับ วิเคราะห์ และคาดการณ์ภัยคุกคามแบบเรียลไทม์ โดยอาศัยโมเดลที่ได้รับการฝึกจากข้อมูลภัย คุกคามในบริบทประเทศไทย [26] [27]

ตารางที่ 1 คำอภิบายการเทคนิค AI ที่ใช้จัดกลุ่มภัยคุกคาม และแนวทางแก้ไข

กลุ่มภัยคุกคามไซเบอร์	เทคนิค AI ที่ใช้จัดกลุ่ม	โมเดล AI	คำอธิบายการประยุกต์ใช้ AI	แนวทางแก้ไข/รับมือ
Malware-Based Attacks	Supervised Learning, Deep Learning	Random Forest, CNN, RNN	วิเคราะห์ไฟล์และพฤติกรรมมัลแวร์เพื่อจำแนกประเภทและตรวจจับมัลแวร์ใหม่	1.ใช้ระบบ Endpoint Protection 2.อัปเดต signature 3.ทำ sandbox analysis
Network-Based Attacks	Unsupervised Learning, Anomaly Detection	K-Means, Autoencoder	ตรวจจับความผิดปกติในทราฟฟิกเครือข่ายและพฤติกรรมที่ไม่ปกติ	1.ติดตั้ง IDS/IPS 2. ทำ network segmentation 3. วิเคราะห์ log แบบ real-time
Application-Level Attacks	NLP, Classification	BERT, Logistic Regression	วิเคราะห์ช่องโหว่และพฤติกรรมการโจมตีแอปพลิเคชัน เช่น SQL Injection, XSS	1.ทำ code review 2. ใช้ WAF 3. อัปเดต patch ซอฟต์แวร์
Social Engineering	NLP, Sentiment Analysis	NLP, Sentiment Analysis	วิเคราะห์ข้อความและพฤติกรรมการหลอกลวง เช่น Phishing, Spear Phishing	1.ฝึกอบรมผู้ใช้ 2.ใช้ email filter 3.ตรวจสอบ URL และ sender
Infrastructure Attacks	Reinforcement Learning	DQN, Policy Gradient	ปรับปรุงการตอบสนองและป้องกันโครงสร้างพื้นฐานสำคัญ เช่น SCADA, IoT	1.แยกเครือข่ายสำคัญ 2.ทำ network monitoring 3.อัปเดต firmware
Strategic and National Attacks	Ensemble Learning, Threat Intelligence	XGBoost, Hybrid Models	วิเคราะห์ภัยคุกคามระดับชาติและการโจมตีแบบซับซ้อนที่มีเป้าหมายเฉพาะ	1.ทำ threat hunting 2.ใช้ threat intelligence sharing 3.วางแผนรับมือเหตุการณ์ระดับชาติ

4. Dashboard เป็นส่วนแสดงผลข้อมูลเชิงวิเคราะห์และการแจ้งเตือนภัยคุกคามต่อผู้ดูแลระบบ โดยเน้น การจัดกลุ่มภัยคุกคามและแนวทางแก้ไข ที่ผ่านการประมวลจากระบบอัจฉริยะ AI / ML Core System [28]



ภาพที่ 4 Dashboard แสดงการจัดกลุ่มภัยคุกคามและแนวทางแก้ไข

ที่ผ่านการประมวลผลจากระบบอัจฉริยะ AI / ML Core System

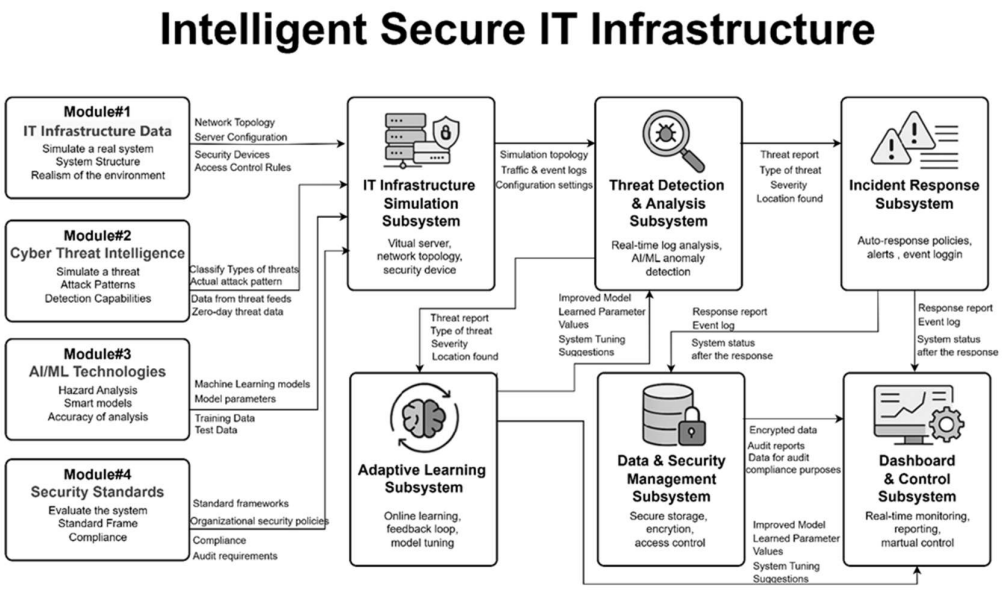
5. Data Knowledge เป็นคลังความรู้ที่รวบรวมข้อมูลภัยคุกคาม รูปแบบการโจมตี และแนวทางการ ตอบสนองที่มีประสิทธิภาพ เพื่อใช้ในการปรับปรุงโมเดล AI/ML และการฝึกอบรมระบบอย่างต่อเนื่อง [29]

กรอบแนวคิดนี้สะท้อนถึงการบูรณาการระหว่างข้อมูลภัยคุกคามในระดับชาติและเทคโนโลยีอัจฉริยะ เพื่อสร้างระบบที่สามารถตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพและทันเวลา โดยเฉพาะในบริบทของโครงสร้างพื้นฐานสำคัญของประเทศไทย [30]

6. วิธีดำเนินการวิจัย

การวิจัยนี้เป็นแบบพัฒนาเชิงทดลอง ผสานการประเมินเชิงทดลอง ภายใต้สภาพแวดล้อมจำลอง ที่แยกจากระบบจริง เพื่อให้ควบคุมตัวแปรได้ ทำซ้ำได้ และลดความเสี่ยงต่อการให้บริการขององค์กรจริง แนวทางใช้ AI/ML สำหรับการตรวจจับ วิเคราะห์ภัยคุกคาม ในเวลาจริง และประเมินผลเทียบกับวิธีดั้งเดิมที่อาศัย signature/rule-based ซึ่งมีข้อจำกัดต่อภัยสมัยใหม่ พร้อมผูกผลการทดลองกับกรอบมาตรฐาน NIST CSF และ ISO/IEC 27001 เพื่อการตรวจสอบและ

นำไปใช้เชิงปฏิบัติได้จริง โดยมีสถาปัตยกรรมของระบบการจำลองสภาพแวดล้อมอัจฉริยะสำหรับการวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ในประเทศไทยตามภาพที่ 5



ภาพที่ 5 สถาปัตยกรรมของระบบการจำลองสภาพแวดล้อมอัจฉริยะสำหรับการวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ในประเทศไทย

ภาพที่ 5 แสดงสถาปัตยกรรมของระบบการจำลองสภาพแวดล้อมอัจฉริยะสำหรับการวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ในประเทศไทย โดยมีส่วนประกอบของระบบแบ่งเป็น 2 ส่วน คือ โมดูลข้อมูลนำเข้า และ ระบบย่อย

6.1 โมดูลข้อมูลนำเข้า จะมี 4 โมดูล ดังนี้

Module#1 IT Infrastructure Data เป็นข้อมูล topology เครือข่าย/เซิร์ฟเวอร์/อุปกรณ์ความปลอดภัย ใช้สร้างสภาพแวดล้อมเสมือนที่ใกล้เคียงระบบจริง

Module#2 Cyber Threat Intelligence เป็นรูปแบบภัยคุกคาม/IOC/TTPs เช่น Malware, Phishing, DDoS, Zero-Day สำหรับป้อนให้เอนจินจำลองการโจมตีและปรับแต่งฉากทดสอบ

Module#3 AI/ML Technologies เป็นโมเดลและพารามิเตอร์ เช่น Random Forest, LSTM, Autoencoder สำหรับงานจำแนกค้นหาผิดปกติ/วิเคราะห์ลำดับเวลา

Module#4 Security Standards เป็นข้อกำหนดควบคุมจาก NIST CSF / ISO/IEC 27001 เพื่อทำ compliance mapping และประเมินความสอดคล้องหลังการทดสอบ

6.2 ระบบย่อย จะมี 6 ระบบ ดังนี้

1. IT Infrastructure Simulation Subsystem ส่งออกโทโพโลยีเสมือน ทราฟฟิก นโยบายความปลอดภัยสำหรับการทดสอบ simulation topology และ config
2. Threat Detection & Analysis Subsystem วิเคราะห์ log/flow แบบเวลาจริง anomaly detection/AI-classification และให้ค่าประเมินสถานะภัยคุกคาม
3. Incident Response Subsystem ใช้ playbooks/SOAR ดำเนินการ block/alert/isolate/log อัตโนมัติ ลดเวลา MTTR และรองรับเวิร์กโฟลว์ IR ตามแนว NIST/ISO
4. Adaptive Learning Subsystem เรียนรู้จากผลทดสอบ เพื่อตั้งค่า และรีเทรนโมเดล ลด Bias ปรับให้ทนต่อภัยคุกคามใหม่ ๆ
5. Data & Security Management Subsystem จัดเก็บข้อมูลทดสอบอย่างปลอดภัย เพื่อรองรับ audit และ compliance
6. Dashboard & Control Subsystem แสดงผลสถานะตัวชี้วัดแบบเวลาจริง ใช้ควบคุมการทดลองและรวบรวมหลักฐานเชิงประจักษ์สำหรับผู้บริหารและผู้เชี่ยวชาญ

6.3 การตั้งค่าสภาพแวดล้อมทดลอง

6.3.1 ออกแบบโทโพโลยีเสมือน โดยให้ เครือข่ายแยกส่วนกัน มีการตั้ง server roles และมีการเพิ่ม security appliances ตาม Module#1 เพื่อสะท้อนโครงสร้างองค์กรทั่วไปในไทย เช่น segmented LAN, DMZ, DC และควบคุมตัวแปรระบบได้ [13] รวมถึงเตรียมข้อมูลการจัดกลุ่มภัยคุกคามที่เกิดขึ้นในประเทศไทย ที่ได้จากการสนทนากลุ่มและการรีวิวจากผู้เชี่ยวชาญป้อนให้ระบบเรียนรู้ในเบื้องต้น

6.3.2 กำหนด Scenario ภัยคุกคาม จาก Module#2 ครอบคลุม Malware Phishing DDoS และ Zero-Day เพื่อทดสอบความยืดหยุ่นของระบบจำลอง [14]

6.3.3 เลือกโมเดล AI/ML จาก Module#3 เช่น Random Forest , LSTM , Autoencoder , Isolation Forest โดยอิงแนวปฏิบัติจากวรรณกรรมทบทวนล่าสุดด้าน AI-based Detection [14]

6.3.4 กำหนดข้อกำหนดมาตรฐาน จาก Module#4 เช่น NIST CSF, ISO/IEC 27001 เพื่อทำการ control mapping และนิยามตัวชี้วัดด้าน compliance ล่วงหน้า [17]

6.4 ขั้นตอนการทดลอง

ขั้นตอนที่ 1 Environment Simulation ปรับใช้ topology/traffic/policies เพื่อตรวจรับรองความสมจริงของสภาพแวดล้อม [13]

ขั้นตอนที่ 2 Attack Simulation จำลองเหตุการณ์โจมตีตามสคริปต์/โปรไฟล์ (threat type, vector, location, duration) เพื่อกระตุ้นข้อมูลจริงสำหรับ AI/ML และเพลย์บุ๊กตอบสนอง [13]

ขั้นตอนที่ 3 Threat Detection & Analysis (AI/ML) ประมวลผล log/flow แบบเวลาจริง โดยจำแนก/ตรวจจับ anomaly และสร้าง Threat report & Severity (ค่าสถานะ สถานที่ เวลาที่ตรวจพบ) ตามกรอบแนวทางรีวิว AI based detection [14]

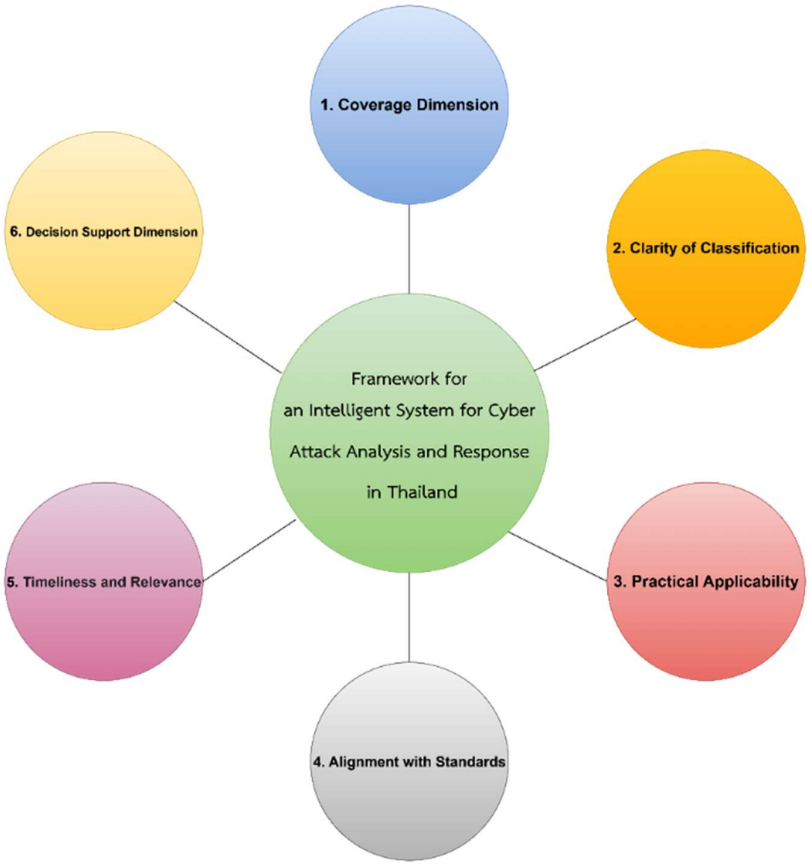
ขั้นตอนที่ 4 Automated Incident Response ทริกเกอร์เพลย์บุ๊ก (block IP, isolate node, elevate alert, forensic log) ตามโมเดลการผสาน NIST และ ISO ในงาน IR สมัยใหม่ [16]

ขั้นตอนที่ 5 Data & Security Management บันทึกข้อมูลทดสอบ ค่าโมเดล ผลลัพธ์อย่างปลอดภัย (encryption + access control) เพื่อรองรับการตรวจสอบย้อนหลังการคำนวณ compliance score [16]

ขั้นตอนที่ 6 Adaptive Learning รีเทรนและฟายน์ทูนโมเดลจากผลทดสอบ เพื่อเพิ่มความแม่นยำ ลด false alarms และปรับตัวต่อภัยใหม่อย่างต่อเนื่อง ตามข้อเสนอของงานทบทวน AI/ML ล่าสุด [14]

ขั้นตอนที่ 7 Dashboard & Reporting สรุปผลการทดลอง accuracy / latency / errors / compliance) และข้อเสนอเชิงวิศวกรรม นโยบายสำหรับผู้ดูแลระบบ ผู้กำกับดูแล [17]

7. ผลการวิจัย



ภาพที่ 6 มิติการประเมินกรอบแนวคิดระบบการจำลองสภาพแวดล้อมอัจฉริยะสำหรับการวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ในประเทศไทย

ภาพที่ 6 แสดงโครงสร้างของมิติการประเมินกรอบแนวคิดระบบการจำลองสภาพแวดล้อมอัจฉริยะสำหรับการวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ในประเทศไทย โดยประกอบด้วย 6 มิติหลักที่เป็นองค์ประกอบสำคัญในการประเมินความเหมาะสมและประสิทธิภาพของกรอบแนวคิด ดังนี้

1. Coverage Dimension (ความครอบคลุม)
   มิตินี้เน้นการประเมินว่ากรอบแนวคิดสามารถครอบคลุมรูปแบบการโจมตีทางไซเบอร์ที่เกิดขึ้นจริงในประเทศไทยได้ครบถ้วนและหลากหลาย

2. Clarity of Classification (ความชัดเจนในการจำแนก)
   มิตินี้ประเมินความชัดเจนในการแบ่งกลุ่มภัยคุกคามและการโจมตี โดยต้องไม่ซ้อนทับกันและสามารถเข้าใจได้ง่าย
3. Practical Applicability (การใช้งานจริง)
   มิตินี้เน้นการประเมินความสามารถในการนำกรอบแนวคิดไปใช้จริงในองค์กร สร้างต้นแบบที่ช่วยลดเวลาความเสียหายและรองรับการกู้คืนระบบได้รวดเร็วขึ้น ในการถูกภัยคุกคามไซเบอร์โจมตี ช่วยผู้ดูแลระบบตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนและ เปลี่ยนแปลงได้อย่างรวดเร็วในโลกปัจจุบัน
4. Alignment with Standards (ความสอดคล้องกับมาตรฐานสากล)
   มิตินี้ประเมินความเชื่อมโยงของกรอบแนวคิดกับมาตรฐานสากล เช่น NIST, MITRE ATT&CK และ Cyber Kill Chain เพื่อให้สามารถบูรณาการกับแนวทางสากลได้
5. Timeliness and Relevance (ความทันสมัยและความเกี่ยวข้อง)
   มิตินี้เน้นการประเมินว่ากรอบแนวคิดสามารถสะท้อนภัยคุกคามที่เกิดขึ้นในปัจจุบันและปรับใช้กับภัยคุกคามใหม่ ๆ ได้อย่างยืดหยุ่น
6. Decision Support Dimension (การสนับสนุนการตัดสินใจ)
   มิตินี้ประเมินความสามารถของกรอบแนวคิดในการสนับสนุนการวางแผนกลยุทธ์ การจัดลำดับความสำคัญ และการกำหนดมาตรการป้องกันและตอบสนองต่อภัยคุกคามไซเบอร์

ภาพนี้ช่วยให้เห็นภาพรวมขององค์ประกอบสำคัญที่ใช้ในการประเมินและพัฒนากรอบแนวคิดระบบการจำลองสภาพแวดล้อมอัจฉริยะสำหรับการวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ในประเทศไทยอย่างเป็นระบบและครบถ้วน

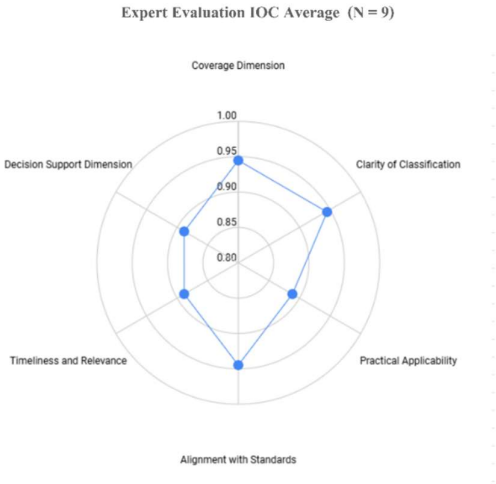
Expert Validation ผู้เชี่ยวชาญประเมิน IOC จำนวน 9 คน

User Validation ผู้ดูแลระบบประเมินกรอบแนวคิด จำนวน 100 คน

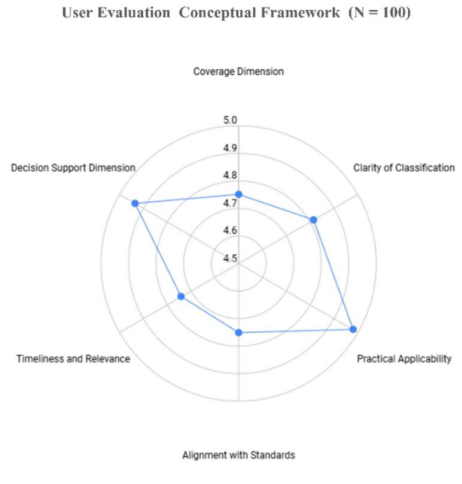
Instruments แบบสอบถามประเมิน IOC และ แบบสอบถามประเมินกรอบแนวคิดโดยใช้ Likert Scale 6 ระดับ ครอบคลุม 6 มิติ ได้แก่ Overage Dimension, Clarity of Classification , Practical Applicability, Alignment with Standards , Timeliness and Relevance และ Decision Support Dimension

Data Analysis ใช้ค่าเฉลี่ย (Mean) ส่วนเบี่ยงเบนมาตรฐาน (S.D.) และ IOC ในการวิเคราะห์ความเหมาะสมของแต่ละมิติและข้อย่อย

Results



ภาพที่ 7 Expert Evaluation IOC Average Conceptual by Dimension (N = 9)



ภาพที่ 8 User Evaluation of Framework Dimension (N = 100)

จากภาพที่ 7 แสดงค่า IOC (Index of Item-Objective Congruence) เฉลี่ย ที่ได้จากการประเมินของผู้เชี่ยวชาญจำนวน 9 คน ใน 6 มิติการประเมินกรอบแนวคิด ประกอบด้วย Coverage Dimension, Clarity of Classification , Practical Applicability, Alignment with Standards , Timeliness and Relevance และ Decision Support Dimension ผลการประเมินพบว่าค่า IOC อยู่ในช่วง 0.85–1.00 โดยเฉพาะมิติ Clarity of Classification , Coverage Dimension และ Alignment with Standards ได้ค่าประเมินสูงสุดใกล้ 1.00 สะท้อนถึงความเห็นพ้องของผู้เชี่ยวชาญในความสอดคล้องของรายการประเมินกับวัตถุประสงค์ของกรอบแนวคิด มิติอื่น ๆ ก็ยังคงอยู่ในระดับสูงเกินเกณฑ์มาตรฐาน (≥ 0.67) แสดงถึงความเชื่อมั่นในความครบถ้วนและความเหมาะสมของกรอบแนวคิด

จากภาพที่ 8 แสดงค่าเฉลี่ยผลการประเมินกรอบแนวคิดจากผู้ดูแลระบบจำนวน 100 คน ครอบคลุม 6 มิติการประเมิน ประกอบด้วย ประกอบด้วย Coverage Dimension, Clarity of Classification , Practical Applicability, Alignment with Standards , Timeliness and Relevance และ Decision Support Dimension พบว่าค่าเฉลี่ยในแต่ละมิติอยู่ในช่วง 4.74–4.97 (จากคะแนนเต็ม 5) โดยมิติ Practical Applicability ได้ค่าเฉลี่ยสูงที่สุด (4.97) รองลงมาคือ Decision Support Dimension แสดงว่าผู้ใช้งานระบบเห็นสอดคล้องกันกรอบแนวคิดสามารถสะท้อนความสามารถของระบบในการใช้งานจริง และสนับสนุนการตัดสินใจได้เป็นอย่างดี ผลลัพธ์ชี้ให้เห็นว่ากรอบแนวคิดที่พัฒนามีความเหมาะสม ครบถ้วน และมีศักยภาพในการนำไปพัฒนา

จากภาพที่ 7 และ 8 เป็นภาพยืนยันความถูกต้องและความน่าเชื่อถือ ของกรอบแนวคิด ในความสอดคล้องเชิงวัตถุประสงค์ (IOC) และความเหมาะสมเชิงคุณภาพ (Mean Score) รายละเอียดตามตารางที่ 2.

ตารางที่ 2 ผลการประเมินความเหมาะสมของกรอบแนวคิดโดยผู้เชี่ยวชาญและผู้ดูแลระบบ

รายการ	$\bar{X}$	S.D.	IOC	ระดับความเหมาะสม
1. Coverage Dimension	4.75	0.42	0.94	มากที่สุด
1.1) กรอบแนวคิดสามารถครอบคลุมรูปแบบการโจมตีทางไซเบอร์ที่เกิดขึ้นจริงในประเทศไทยได้	4.84	0.37	1.00	มากที่สุด
1.2) กลุ่มการโจมตีที่กำหนดสามารถสะท้อนภัยคุกคามที่หลากหลายได้ครบถ้วน	4.66	0.48	0.89	มากที่สุด
2. Clarity of Classification	4.81	0.39	0.94	มากที่สุด
2.1) การแบ่งกลุ่มการโจมตีมีความชัดเจน ไม่ซ้อนทับกัน และเข้าใจง่าย	4.85	0.36	0.89	มากที่สุด
2.2) ภัยคุกคามในแต่ละกลุ่มมีลักษณะร่วมกันอย่างเป็นระบบ	4.78	0.42	1.00	มากที่สุด
3. Practical Applicability	4.98	0.14	0.89	มากที่สุด
3.1) กรอบแนวคิดสามารถนำไปใช้ในการวิเคราะห์หรือจัดการภัยคุกคามในองค์กรได้จริง	4.98	0.14	0.89	มากที่สุด
3.2) กรอบแนวคิดเหมาะสมกับการใช้ในการอบรมหรือจัดทำรายงานด้านไซเบอร์	4.98	0.14	0.89	มากที่สุด
4. Alignment with Standards	4.75	0.43	0.94	มากที่สุด
4.1) กรอบแนวคิดมีความเชื่อมโยงกับมาตรฐานสากล เช่น NIST, MITRE ATT&CK, Cyber Kill Chain	4.69	0.47	0.89	มากที่สุด
4.2) กรอบแนวคิดสามารถบูรณาการร่วมกับโมเดลหรือกรอบการวิเคราะห์อื่นได้	4.81	0.40	1.00	มากที่สุด
5. Timeliness and Relevance	4.75	0.40	0.89	มากที่สุด
5.1) กรอบแนวคิดสะท้อนภัยคุกคามที่เกิดขึ้นในปัจจุบันและแนวโน้มในอนาคตได้	4.89	0.31	0.89	มากที่สุด
5.2) กรอบแนวคิดสามารถปรับใช้กับภัยคุกคามใหม่ ๆ ได้อย่างยืดหยุ่น	4.61	0.49	0.89	มากที่สุด
6. Decision Support Dimension	4.84	0.24	0.89	มากที่สุด
6.1) กรอบแนวคิดสามารถใช้ในการวางแผนกลยุทธ์และการจัดลำดับความสำคัญด้านไซเบอร์ได้	4.92	0.27	0.89	มากที่สุด
6.2) กรอบแนวคิดสามารถใช้ในการกำหนดมาตรการป้องกันและตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพ	4.76	0.22	0.89	มากที่สุด
สรุปภาพรวม	4.81	0.34	0.91	มากที่สุด

จากตารางที่ 2 ผลการประเมินจากผู้เชี่ยวชาญจำนวน 9 คนและผู้ดูแลระบบจำนวน 100 คน ต่อกรอบแนวคิดการพัฒนาระบบอัจฉริยะ พบว่าค่าเฉลี่ยรวมทั้ง 6 มิติอยู่ในระดับมากที่สุด ($\bar{X}$ รวม = 4.81, S.D. = 0.34, IOC = 0.91) สะท้อนว่ากรอบแนวคิดมีความครบถ้วน เหมาะสม และสามารถนำไปใช้ในการพัฒนาต้นแบบระบบอัจฉริยะได้จริง รายละเอียดผลการประเมินรายมิติ ดังนี้ **1) Coverage Dimension** ผลการประเมินด้านความครอบคลุมของระบบได้ค่าเฉลี่ย $\bar{X}$ = 4.75 (S.D. = 0.42, IOC = 0.94) อยู่ในระดับมากที่สุด โดยผู้เชี่ยวชาญและผู้ดูแลระบบเห็นว่ากรอบแนวคิดมีองค์ประกอบครอบคลุมรูปแบบการโจมตีทางไซเบอร์ที่เกิดขึ้นจริงในประเทศไทย และกลุ่มการโจมตีที่กำหนดสามารถสะท้อนภัยคุกคามที่หลากหลายได้ครบถ้วน **2) Clarity of Classification** ด้านความชัดเจนในการจำแนกได้ค่าเฉลี่ยระดับมากที่สุด เป็นลำดับสาม ($\bar{X}$ = 4.81, S.D. = 0.39, IOC = 0.94) ผู้เชี่ยวชาญและผู้ดูแลระบบประเมินว่าการแบ่งกลุ่มการโจมตีมีความชัดเจน ไม่ซ้อนทับกัน และเข้าใจง่ายภัยคุกคามในแต่ละกลุ่มมีลักษณะร่วมกันอย่างเป็นระบบ **3) Practical Applicability** ผลการประเมินการใช้งานจริงมีค่าเฉลี่ยสูงสุด $\bar{X}$ = 4.98 (S.D. = 0.14, IOC = 0.89) อยู่ในระดับมากที่สุด เป็นอันดับที่หนึ่ง โดยผู้เชี่ยวชาญและผู้ดูแลระบบเห็นว่ากรอบแนวคิดสามารถนำไปใช้ในการวิเคราะห์ หรือจัดการภัยคุกคามในองค์กรได้จริง และกรอบแนวคิดเหมาะสมกับการใช้ในการอบรมหรือจัดทำรายงานด้านไซเบอร์ **4) Alignment with Standards** ด้านความสอดคล้องกับมาตรฐานสากลได้ค่าเฉลี่ยระดับมากที่สุด ($\bar{X}$ = 4.75, S.D. = 0.43, IOC = 0.94) ผู้เชี่ยวชาญและผู้ดูแลระบบประเมินว่ากรอบแนวคิดมีความเชื่อมโยงกับมาตรฐานสากล กรอบแนวคิดสามารถบูรณาการร่วมกับโมเดลหรือกรอบการวิเคราะห์อื่นได้ **5) Timeliness and Relevance** ผลการประเมินด้านความทันสมัยและความเกี่ยวข้องได้ค่าเฉลี่ย $\bar{X}$ = 4.75 (S.D. = 0.40, IOC = 0.89) อยู่ในระดับมากที่สุด ผู้เชี่ยวชาญและผู้ดูแลระบบยืนยันว่ากรอบแนวคิดสามารถสะท้อนภัยคุกคามที่เกิดขึ้นในปัจจุบันและแนวโน้มในอนาคตได้ สามารถปรับใช้กับภัยคุกคามใหม่ ๆ ได้อย่างยืดหยุ่น **6) Decision Support Dimension** ด้านการสนับสนุนการตัดสินใจได้ค่าเฉลี่ยระดับมากที่สุด เป็นลำดับสอง ($\bar{X}$ = 4.84, S.D. = 0.24, IOC = 0.89) ผู้เชี่ยวชาญและผู้ดูแลระบบประเมินว่ากรอบแนวคิดสามารถใช้ในการวางแผนกลยุทธ์และการจัดลำดับความสำคัญด้านไซเบอร์ได้ สามารถใช้ในการกำหนดมาตรการป้องกันและตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพ

จากผลการประเมิน พบว่ากรอบแนวคิดที่พัฒนามีความเหมาะสมในทุกมิติ โดยเฉพาะ Practical Applicability ซึ่งสะท้อนศักยภาพนำไปใช้ในการวิเคราะห์ หรือจัดการภัยคุกคามในองค์กรได้จริง ขณะที่มิติอื่น ๆ ได้แก่ Decision Support Dimension , Clarity of Classification , Coverage Dimension , Alignment with Standards และ Timeliness and Relevance ต่างก็ได้รับการประเมินในระดับมากที่สุด สรุปได้ว่ากรอบแนวคิดนี้เป็นรากฐานที่แข็งแรงทั้งด้านทฤษฎีและการนำไปประยุกต์ใช้จริง สามารถรองรับการพัฒนาต้นแบบระบบอัจฉริยะที่มีความแม่นยำ โปร่งใส และเน้นผู้ใช้เป็นศูนย์กลางได้อย่างยั่งยืน

8. สรุปแนวคิดการวิจัย

งานวิจัยนี้ได้พัฒนา สภาพแวดล้อมจำลองอัจฉริยะ (Intelligent Secure IT Infrastructure Simulation Environment) ที่ผสานทฤษฎีระบบจำลอง เทคโนโลยี AI/ML และกรอบมาตรฐานความมั่นคงปลอดภัยไซเบอร์ เพื่อรองรับการวิเคราะห์และตอบสนองต่อภัยคุกคามยุคใหม่ที่มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว ซึ่งระบบความปลอดภัยแบบดั้งเดิมไม่สามารถตอบสนองได้ทันเวลา [14]

“ประเด็นสำคัญที่สุด และ จุดประสงค์หลัก ของการวิจัยนี้ คือ เพื่อช่วยลดเวลาความเสียหาย (Damage Time) และรองรับการกู้คืนระบบ (System Recovery) ให้เร็วขึ้นเมื่อเกิดการโจมตีทางไซเบอร์ ผ่านการมีต้นแบบระบบจำลองที่สามารถนำไปประยุกต์ใช้จริงในองค์กร และช่วยผู้ดูแลระบบตรวจจับตอบสนองภัยคุกคามได้ทันท่วงทีและมีประสิทธิภาพมากขึ้น”

จุดประสงค์นี้เป็นแก่นสำคัญที่ตอบโจทย์ความท้าทายของภัยคุกคามไซเบอร์ปัจจุบัน ซึ่งสามารถโจมตีแบบอัตโนมัติ เคลื่อนไหวรวดเร็ว และมีลักษณะซับซ้อน เช่น APT, Zero day, AI assisted attacks ตามที่งานวิจัยสากลรายงานไว้หลายฉบับ [13]

8.1 การอภิปราย

ผลการประเมินโดยผู้เชี่ยวชาญจำนวน 9 คน และผู้ดูแลระบบจำนวน 100 คน ชี้ให้เห็นว่ากรอบแนวคิดการพัฒนาระบบอัจฉริยะสำหรับการวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ในประเทศไทย มีความเหมาะสมในระดับมากที่สุดทุกมิติ ทั้งด้านความครอบคลุม ความชัดเจนในการจำแนก การใช้งานจริง ความสอดคล้องกับมาตรฐานสากล ความทันสมัย และการสนับสนุนการตัดสินใจ โดยเฉพาะ Practical Applicability ที่ได้รับคะแนนสูงสุด แสดงถึงศักยภาพในการนำไปใช้จริงในองค์กรและการฝึกอบรมบุคลากรด้านความมั่นคงไซเบอร์ กรอบแนวคิดนี้สอดคล้องกับหลักการของ System Theory[31], Agent Theory[32], Learning Theory[33, 34]และ XAI Theory[35] ซึ่งเน้นความเป็นองค์รวม การเรียนรู้เชิงประสบการณ์ และความโปร่งใสในการตัดสินใจของระบบอัจฉริยะ ผลการประเมินในแต่ละมิติ เช่น Coverage Dimension, Clarity of Classification, Practical Applicability, Alignment with Standards , Timeliness and Relevance และ Decision Support Dimension ล้วนได้รับการยืนยันจากผู้เชี่ยวชาญว่ามีความเหมาะสมและสามารถนำไปประยุกต์ใช้ได้จริง กรอบแนวคิดที่นำเสนอสามารถนำไปใช้เป็นแนวทางในการพัฒนาต้นแบบระบบอัจฉริยะสำหรับการวิเคราะห์และตอบสนองต่อภัยคุกคามไซเบอร์ในประเทศไทยได้อย่างมีประสิทธิภาพ ทั้งในระดับองค์กรและระดับประเทศ นอกจากนี้ยังสามารถต่อยอดสู่การพัฒนา

เครื่องมือสนับสนุนการตัดสินใจ และระบบฝึกอบรมบุคลากรด้านความมั่นคงไซเบอร์ แม้กรอบแนวคิดจะได้รับการประเมินในระดับสูง แต่ยังมีข้อจำกัดบางประการ เช่น การปรับใช้กับภัยคุกคามรูปแบบใหม่ที่เกิดขึ้นอย่างรวดเร็ว หรือข้อจำกัดด้านข้อมูลสำหรับการฝึกโมเดล AI/ML ในบริบทประเทศไทย ดังนั้นการพัฒนาต่อไปควรเน้นการบูรณาการข้อมูลจากหลายแหล่ง การปรับปรุงโมเดลให้รองรับภัยคุกคามใหม่ ๆ และการสร้างกลไกการเรียนรู้แบบต่อเนื่อง เพื่อเพิ่มประสิทธิภาพของระบบในระยะยาว ควรมีการสนับสนุนเชิงนโยบายในการนำกรอบแนวคิดนี้ไปใช้จริงในหน่วยงานภาครัฐและเอกชน รวมถึงการส่งเสริมความร่วมมือระหว่างภาคส่วนต่าง ๆ ในการแลกเปลี่ยนข้อมูลภัยคุกคามและแนวทางปฏิบัติที่ดี นอกจากนี้ควรมีการวิจัยต่อยอดในด้าน Explainable AI (XAI) เพื่อเพิ่มความโปร่งใสและความน่าเชื่อถือของระบบอัจฉริยะในงานด้านความมั่นคงไซเบอร์

8.1 สรุปและงานวิจัยในอนาคต

งานวิจัยนี้นำเสนอกรอบแนวคิดระบบอัจฉริยะสำหรับการวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ในประเทศไทย โดยอาศัยการจำแนกประเภทภัยคุกคามที่เกิดขึ้นจริงในบริบทระดับชาติ กรอบแนวคิดที่พัฒนาขึ้นประกอบด้วยองค์ประกอบหลัก ได้แก่ การรวบรวมข้อมูลเหตุการณ์ไซเบอร์ (Data Log) การจำแนกภัยคุกคามตามหมวดหมู่ที่เหมาะสมกับบริบทประเทศไทย การวิเคราะห์ด้วยระบบ AI/ML การแสดงผลผ่าน Dashboard และการจัดเก็บองค์ความรู้เพื่อการเรียนรู้และปรับปรุงระบบอย่างต่อเนื่อง ผลการประเมินจากผู้เชี่ยวชาญและผู้ดูแลระบบ พบว่ากรอบแนวคิดนี้มีความเหมาะสมในทุกมิติ ทั้งด้านความครอบคลุม ความชัดเจนในการจำแนก การใช้งานจริง ความสอดคล้องกับมาตรฐานสากล ความทันสมัยและความเกี่ยวข้อง ตลอดจนการสนับสนุนการตัดสินใจ โดยเฉพาะ Practical Applicability ที่ได้รับคะแนนสูงสุด สะท้อนถึงศักยภาพในการนำไปใช้จริงในองค์กรและระดับประเทศ ระบบอัจฉริยะที่ออกแบบขึ้นสามารถตรวจจับและตอบสนองต่อภัยคุกคามแบบเรียลไทม์ได้อย่างมีประสิทธิภาพ โดยอาศัยเทคนิคการเรียนรู้ของเครื่องที่ทันสมัย เช่น Supervised Learning, Deep Learning และ Reinforcement Learning ซึ่งได้รับการพิสูจน์แล้วว่ามีประสิทธิภาพในการวิเคราะห์ภัยคุกคามที่ซับซ้อน โดยสรุปกรอบแนวคิดนี้ถือเป็นรากฐานสำคัญสำหรับการพัฒนาต้นแบบระบบอัจฉริยะที่มีความแม่นยำ โปร่งใส และเน้นผู้ใช้เป็นศูนย์กลาง สามารถนำไปประยุกต์ใช้ในการวางแผนกลยุทธ์ การฝึกอบรม และการพัฒนาระบบป้องกันภัยคุกคามไซเบอร์ในโครงสร้างพื้นฐานสำคัญของประเทศไทยได้อย่างยั่งยืน

แม้ว่างานวิจัยนี้จะประสบความสำเร็จในการพัฒนากรอบแนวคิดที่เหมาะสมกับบริบทของประเทศไทย แต่ยังมีประเด็นสำคัญที่ควรศึกษาและพัฒนาต่อยอดในอนาคต ดังนี้

1. การพัฒนาต้นแบบและทดสอบในสภาพแวดล้อมจริง ควรดำเนินการพัฒนาต้นแบบระบบอัจฉริยะตามกรอบแนวคิดที่นำเสนอ และทดสอบในสภาพแวดล้อมจริงขององค์กรและโครงสร้างพื้นฐานสำคัญ เพื่อประเมินประสิทธิภาพและความสามารถในการตรวจจับและตอบสนองต่อภัยคุกคามที่เกิดขึ้นจริง

2. การบูรณาการกับเทคโนโลยีเกิดใหม่ ศึกษาการบูรณาการเทคโนโลยีใหม่ เช่น Blockchain, IoT Security, Federated Learning และ XAI (Explainable AI) เพื่อเพิ่มขีดความสามารถของระบบในการรับมือกับภัยคุกคามที่มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว
3. การพัฒนาโมเดล AI ที่ปรับตัวได้อัตโนมัติ วิจัยและพัฒนาโมเดล AI/ML ที่สามารถเรียนรู้จากข้อมูลภัยคุกคามใหม่ ๆ และปรับปรุงกลยุทธ์การตรวจจับและตอบสนองได้แบบอัตโนมัติ (Adaptive Learning) เพื่อรองรับภัยคุกคามรูปแบบใหม่ที่เกิดขึ้นอย่างต่อเนื่อง
4. การสร้างกลไกการแบ่งปันข้อมูลภัยคุกคามอย่างปลอดภัย พัฒนาแนวทางและมาตรการสำหรับการแบ่งปันข้อมูลภัยคุกคาม (Threat Intelligence Sharing) ระหว่างองค์กรและหน่วยงานภาครัฐ/เอกชน เพื่อเสริมสร้างความร่วมมือและการป้องกันภัยคุกคามในระดับประเทศ
5. การศึกษาประเด็นด้านจริยธรรม กฎหมาย และนโยบาย วิเคราะห์ผลกระทบด้านจริยธรรม กฎหมาย และนโยบายที่เกี่ยวข้องกับการนำ AI/ML ไปใช้ในระบบความมั่นคงไซเบอร์ เพื่อให้เกิดการใช้งานอย่างรับผิดชอบ โปร่งใส และสอดคล้องกับมาตรฐานสากล
6. การประเมินผลกระทบและความคุ้มค่าทางเศรษฐกิจ ศึกษาผลกระทบและความคุ้มค่าทางเศรษฐกิจจากการนำระบบอัจฉริยะไปใช้ในองค์กรและระดับประเทศ เพื่อสนับสนุนการตัดสินใจลงทุนและการกำหนดนโยบายในอนาคต

การดำเนินการวิจัยและพัฒนาต่อยอดในประเด็นข้างต้น จะช่วยเสริมสร้างศักยภาพของระบบอัจฉริยะสำหรับการวิเคราะห์และตอบสนองต่อการโจมตีทางไซเบอร์ในประเทศไทยให้มีความยั่งยืนและทันสมัย รองรับภัยคุกคามที่เปลี่ยนแปลงอย่างต่อเนื่องในยุคดิจิทัล

9. เอกสารอ้างอิง

[1] Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data 2024 11:1*, *11*(1), 105-. https://doi.org/10.1186/S40537-024-00957-Y

[2] 2025 Data Breach Investigations Report | Verizon. (n.d.). Retrieved January 25, 2026, from https://www.verizon.com/business/resources/reports/dbir/

[3] Kutagamari, V. (2025). Issue 3 | www.ijedr.org IJEDR2503053. *International Journal of Engineering Development and Research*, *13*, 528. Retrieved from www.ijedr.org

[4] Jaber, A., & Fritsch, L. (2023). Towards AI-powered Cybersecurity Attack Modeling with Simulation Tools: Review of Attack Simulators. *Lecture Notes in Networks and Systems*, *571 LNNS*, 249–257. https://doi.org/10.1007/978-3-031-19945-5_25

[5] Md Abu Imran Mallick, & Rishab Nath. (2024). (PDF) Simulating Cyber Threats: A Review of AI-powered Attack Simulators for Enhanced Cybersecurity. *World Scientfic News*. Retrieved January 25, 2026, from https://www.researchgate.net/publication/384286062_Simulating_Cyber_Threats_A_Review_of_AI-powered_Attack_Simulators_for_Enhanced_Cybersecurity

[6] Banks, J. , Carson, J. S. , Nelson, B. L., & and Nicol, D. M. (2010). Banks, J., Carson, J.S., Nelson, B.L. and Nicol, D.M. (2010) Discrete-Event System Simulation. 5th Edition, Pearson Education, New Delhi. - References - Scientific Research Publishing. Retrieved January 25, 2026, from https://www.researchgate.net/publication/234125560_Discret-Event_System_Simulation

[7] Lokare, A., Shripad Bankar, U., & Padmajeet Mhaske JPMC, U. (n.d.). Integrating Cybersecurity Frameworks into IT Security: A Comprehensive Analysis of Threat Mitigation Strategies and Adaptive Technologies.

[8] Akpan Essien, I., Cadet, E., Ajayi, J. O., Erigha, D., & Obuse, E. (2020). Cyber Risk Mitigation and Incident Response Model Leveraging ISO 27001 and NIST for Global Enterprises.

[9] Vassilev, A., Oprea, A., Fordyce, A., Anderson, H., Davies, X., & Hamin, M. (n.d.). NIST Trustworthy and Responsible AI NIST AI 100-2e2025 Adversarial Machine Learning A Taxonomy and Terminology of Attacks and Mitigations. https://doi.org/10.6028/NIST.AI.100-2e2025

[10] Mallick, A. I., & Nath, R. (2024). Simulating Cyber Threats: A Review of AI-powered Attack Simulators for Enhanced Cybersecurity. *World Scientific News*.

[11] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (2018). https://doi.org/10.6028/NIST.CSWP.04162018

[12] Tallam EECS, K. (2025). Transforming Cyber Defense: Harnessing Agentic and Frontier AI for Proactive, Ethical Threat Intelligence.

[13] ISO 42001 + ISO 27001: AI Cybersecurity Framework Guide. (n.d.). Retrieved January 28, 2026, from https://digital.nemko.com/insights/iso-42001-ai-cybersecurity-complete-implementation-guide

[14] AI-Aware Cyber Range Simulations | Cloud Range Live-Fire SOC Training | Cloud Range. (n.d.). Retrieved January 28, 2026, from https://www.cloudrangecyber.com/cyber-ai-simulations

[15] Cyber Range Platform: Real Training Scenarios & Simulations. (n.d.). Retrieved January 28, 2026, from https://www.cyberbit.com/product/cyber-range/

[16] ISO/IEC DIS 27090 - Cybersecurity — Artificial Intelligence — Guidance for addressing security threats and compromises to artificial intelligence systems. (n.d.). Retrieved January 28, 2026, from https://www.iso.org/standard/56581.html

[17] AI Research - Security and Resilience | NIST. (n.d.). Retrieved January 28, 2026, from https://www.nist.gov/artificial-intelligence/ai-research-security-and-resilience

[18] Junklewitz, H., Hamon, R., & Sanchez, I. (n.d.). Addressing AI cybersecurity requirements.

[19] Thomas Rid. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies*. https://doi.org/10.1080/01402390.2011.608939

[20] Healey, J. (2013). A fierce domain : conflict in cyberspace, 1986 to 2012. *CiNii Research*. Retrieved from https://cir.nii.ac.jp/crid/1970586434873253964

[21] Brantly, A. F. (2021). *The Cyber Deterrence Problem*.

[22] Gupta, S., & Gupta, B. B. (2017). Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. *International Journal of System Assurance Engineering and Management*, *8*(1), 512–530. https://doi.org/10.1007/S13198-015-0376-0/TABLES/7

[23] Gao, J., Li, L., Kong, P., Bissyande, T. F., & Klein, J. (2019). Should You Consider Adware as Malware in Your Study? *SANER 2019 - Proceedings of the 2019 IEEE 26th International Conference on Software Analysis, Evolution, and Reengineering*, 604–608. https://doi.org/10.1109/SANER.2019.8668010

[24] Park, J. H., Singh, S. K., Salim, M. M., Azzaoui, A. E. L., & Park, J. H. (2022). Ransomware-based Cyber Attacks: A Comprehensive Survey. *Journal of Internet Technology*, *23*(7), 1557–1564. https://doi.org/10.53106/160792642022122307010

[25] Thomas, K., Pullman, J., Yeo, K., Raghunathan, A., Gage Kelley, P., Invernizzi, L., … Boneh Elie Bursztein, D. (n.d.). Protecting accounts from credential stuffing with password breach alerting. Retrieved from https://www.usenix.org/conference/usenixsecurity19/presentation/thomas

[26] Cybersecurity Frameworks Comparison: 10 Common Frameworks - Tolu Michael. (n.d.). Retrieved September 19, 2025, from https://tolumichael.com/cybersecurity-frameworks-comparison/

[27] Ovabor, K., Oluwatobiloba Sule-Odu, I., Atkison, T., Fabusoro, A. T., & Benedict, J. O. (2024). Corresponding author: Ismail Oluwatobiloba Sule-Odu AI-driven threat intelligence for real-time cybersecurity: Frameworks, tools, and future directions. *Open Access Research Journal of Science and Technology*, *2024*(02), 40–048. https://doi.org/10.53022/oarjst.2024.12.2.0135

[28] Olafuyi, B. A. (2023). Artificial Intelligence in Cybersecurity: Enhancing Threat Detection and Mitigation. *International Journal of Scientific and Research Publications*, *13*(12). https://doi.org/10.29322/IJSRP.13.12.2023.p14419

[29] Yang, J., Chouchane, R., Ge, L., Bernardo, L., Malta, S., & Magalhães, J. (2025). An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF. *Electronics 2025, Vol. 14, Page 1364*, *14*(7), 1364. https://doi.org/10.3390/ELECTRONICS14071364

[30] Feature Article: Leveraging AI to Enhance the Nation's Cybersecurity | Homeland Security. (n.d.). Retrieved September 19, 2025, from https://www.dhs.gov/science-and-technology/news/2024/10/17/feature-article-leveraging-ai-enhance-nations-cybersecurity

[31] Chen, F., Wang, Z., & Yang, X. (2025). Intelligent System Architecture Based on System Theory. *Chinese Journal of Information Fusion*, *2*(1), 1–13. https://doi.org/10.62762/CJIF.2024.872211

[32] What Is a keylogger and how to detect keystroke logging - Norton. (n.d.). Retrieved September 18, 2025, from https://us.norton.com/blog/malware/what-is-a-keylogger

[33] Gibson, D., Kovanovic, V., Ifenthaler, D., Dexter, S., & Feng, S. (2023). Learning theories for artificial intelligence promoting learning processes. *British Journal of Educational Technology*, *54*(5), 1125–1146. https://doi.org/10.1111/BJET.13341

[34] Parmar, B. (2012). Protecting against spear-phishing. *Computer Fraud & Security*, *2012*(1), 8–11. https://doi.org/10.1016/S1361-3723(12)70007-6

[35] Phishing Detection: A Literature Survey | IEEE Journals & Magazine | IEEE Xplore. (n.d.). Retrieved September 18, 2025, from https://ieeexplore.ieee.org/abstract/document/6497928?casa_token=zquBayiwIIIAAAAA:DdfqlG7n_2zosPt_iFxxx6ui_BUQXuftZnKGzkzdBqfXgFpGM9oMCFd5rMwQFGjJrR0xeHCSbTE

Plagiarism Checking Report

Created on 2026-01-28 23:06:07 at 23:06 PM

Submission Information

ID	SUBMISSION DATE	SUBMITTED BY	ORGANIZATION	FILENAME	STATUS	SIMILARITY INDEX
4607022	Jan 28, 2026 at 23:01 PM	168490432006-st@rmutsb.ac.th	มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ	DMT ปริญญาเอก ชั้นปีที่1 นายอนุรักษ์ ดันตราธิปไตย The 3st Digital Media Technology Graduate Seminar.pdf	Completed	0.00 %

Match Overview

NO.	TITLE	AUTHOR(S)	SOURCE	SIMILARITY INDEX
No data available in table				