การปรับปรุงประสิทธิภาพการตอบสนองต่อภัยคุกคามไซเบอร์ด้วยวัฏจักร PDCA: การบูรณาการระบบตรวจจับ (Wazuh IDS) และระบบอัตโนมัติแปลผลด้วยปัญญาประดิษฐ์ (n8n/AI)

นายนัทธพงศ์ วิวิธสุรการ

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2568
ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

การปรับปรุงประสิทธิภาพการตอบสนองต่อภัยคุกคามไซเบอร์ด้วยวัฏจักร PDCA: การบูรณาการระบบตรวจจับ (Wazuh IDS) และระบบอัตโนมัติแปลผลด้วยปัญญาประดิษฐ์ (n8n/AI)

นายนัทธพงศ์ วิวิธสุรการ

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2568
ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ



ใบรับรองการค้นคว้าอิสระ

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง การปรับปรุงประสิทธิภาพการตอบสนองต่อภัยคุกคามไซเบอร์ด้วยวัฏจักร PDCA: การบูรณาการระบบตรวจจับ (Wazuh IDS) และระบบอัตโนมัติแปลผลด้วยปัญญาประดิษฐ์ (n8n/AI)

โดย นายนัทธพงศ์ วิวิธสุรการ

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ

คณบดีคณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล

.....

(ผู้ช่วยศาสตราจารย์ ดร.สุนันฑา สดสี)

คณะกรรมการสอบการค้นคว้าอิสระ

.....

ประธาน

(รองศาสตราจารย์ ดร.สุมิตรา นวลมีศรี)

.....

อาจารย์ที่ปรึกษา

(ผู้ช่วยศาสตราจารย์ ดร.สุนันฑา สดสี)

.....

กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์)

ชื่อ : นายนัทธพงศ์ วิวิธสุรการ

ชื่อการค้นคว้าอิสระ : การปรับปรุงประสิทธิภาพการตอบสนองต่อภัยคุกคามไซเบอร์ด้วยวัฏจักร PDCA: การบูรณาการระบบตรวจจับ (Wazuh IDS) และระบบอัตโนมัติแปลผลด้วยปัญญาประดิษฐ์ (n8n/AI)

สาขาวิชา : การบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก : ผู้ช่วยศาสตราจารย์ ดร.สุนันฑา สดสี

ปีการศึกษา : 2568

บทคัดย่อ

ในปัจจุบันภัยคุกคามทางไซเบอร์มีความซับซ้อนและเพิ่มจำนวนขึ้นอย่างต่อเนื่องแต่ระบบรักษาความปลอดภัยระดับองค์กรส่วนใหญ่มักมีความซับซ้อน มีค่าใช้จ่ายสูงและต้องพึ่งพาผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์โดยตรงทำให้ผู้ใช้งานทั่วไป (เช่น ผู้ใช้ตามบ้าน หรือองค์กรขนาดเล็กที่ไม่มีทีม IT) ไม่สามารถเข้าถึงหรือใช้งานระบบป้องกันภัยที่มีประสิทธิภาพได้ด้วยตนเอง งานวิจัยนี้มีวัตถุประสงค์เพื่อ ก) พัฒนาและบูรณาการระบบต้นแบบสำหรับตรวจจับภัยคุกคามไซเบอร์ใช้ Wazuh IDS ร่วมกับระบบ Automation n8n และปัญญาประดิษฐ์ (AI) ในการแปลผลและสรุปการแจ้งเตือนภัยคุกคามให้เข้าใจง่าย และ ข) ประเมินประสิทธิภาพของระบบที่พัฒนาขึ้นและปรับปรุงประสิทธิภาพการตอบสนองของผู้ใช้งานทั่วไปต่อภัยคุกคามไซเบอร์อย่างต่อเนื่อง ผ่านการประยุกต์ใช้วัฏจักร PDCA (Plan, Do, Check, Act) งานวิจัยนี้ใช้วิธีการวิจัยเชิงปฏิบัติการมีวัฏจักร PDCA เป็นกรอบการดำเนินงานหลักในการปรับปรุงอย่างต่อเนื่อง ระบบต้นแบบจะทำหน้าที่รับการแจ้งเตือนทางเทคนิคจาก Wazuh IDS แล้วส่งต่อผ่าน n8n ไปยังโมเดล AI เพื่อแปลผลเป็นข้อความแจ้งเตือนที่กระชับ ชัดเจน และให้คำแนะนำที่ต้องดำเนินการทันทีกลุ่มตัวอย่างที่เป็นพนักงาน/ผู้ใช้งานทั่วไปจำนวน 25 คน การวัดผลแบ่งออกเป็นสองด้านหลัก ได้แก่ เกณฑ์วัดผลด้านระบบ (System Metrics) ซึ่งรวมถึง Precision, Recall, F1-score และ Detection Time และเกณฑ์วัดผลด้านผู้ใช้งาน (User Metrics) ซึ่งวัดจาก User Response Time, Correct Response Rate และ Security Awareness Score จากการเปรียบเทียบผล Pre-test/ Post-test ผลการทดลองแสดงให้เห็นว่าระบบบูรณาการนี้มีประสิทธิภาพทางเทคนิคสูงมีค่า Precision, Recall และ F1-score เท่ากับ 1.0 (100%) และเวลา

ในการตรวจจับเฉลี่ยอยู่ที่ประมาณ 5.31 วินาที ในด้านผู้ใช้งาน พบว่าคะแนนเฉลี่ยความตระหนักรู้ด้านความปลอดภัยเพิ่มขึ้น

อย่างมีนัยสำคัญจาก 6.88 เป็น 16.84 คะแนนหลังการทดลอง และค่าส่วนเบี่ยงเบนมาตรฐานลดลงอย่างชัดเจน ซึ่งยืนยันว่าการใช้ระบบแจ้งเตือนที่แปลผลด้วย AI และการดำเนินการปรับปรุงอย่างเป็นระบบตามวัฏจักร PDCA สามารถลดช่องว่างด้านความรู้ เพิ่มความเข้าใจในภัยคุกคาม และพัฒนาประสิทธิภาพการตอบสนองต่อภัยคุกคามไซเบอร์ของผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญได้อย่างชัดเจน งานวิจัยนี้ได้สร้างแนวทางปฏิบัติที่ชัดเจนในการบูรณาการเครื่องมือ Open-Source เพื่อสร้าง เครื่องมือ Workflow Automation แบบ Real-time ที่สามารถนำไปประยุกต์ใช้ได้ในองค์กรขนาดเล็ก

(มีจำนวนทั้งสิ้น 58 หน้า)

คำสำคัญ : ภัยคุกคามไซเบอร์ ระบบตรวจจับ (Wazuh IDS + AI) Workflow Automation (n8n + PDCA)

_____ อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก

Name : Mr. Nutthapong Vivithsurakarn
Independent Study Title : Improving Cybersecurity Response Efficiency using the PDCA Cycle: Integrating Intrusion Detection Systems (Wazuh IDS) and AI-Assisted Automated Alert Translation (n8n/AI)
Major Field : Digital Network and Information Security Management
King Mongkut's University of Technology North Bangkok
Independent Study Advisor : Assistant Professor Dr. Sunantha Sodsee
Academic Year : 2025

ABSTRACT

Currently, cyber threats are becoming increasingly complex and continuous, yet most enterprise-level security systems remain complicated, costly, and heavily reliant on IT and cybersecurity experts. This creates a significant barrier for general users, such as home users or small organizations without dedicated IT teams, preventing them from accessing or managing effective defense systems independently. This research aims to develop and integrate a prototype cyber threat detection system using Wazuh IDS in conjunction with the n8n automation platform and Artificial Intelligence (AI) to interpret and summarize threat alerts into an easily understandable format, while also evaluating the system's performance and continuously improving user response efficiency through the application of the PDCA (Plan-Do-Check-Act) cycle. Adopting an action research methodology, the prototype functions by receiving technical alerts from Wazuh IDS, which are then routed through n8n to an AI model to be translated into concise notifications with immediate actionable advice for a sample group of 25 general users. Performance was measured across system metrics (Precision, Recall, F1-score, and Detection Time) and user metrics (User Response Time, Correct Response Rate, and Security Awareness Scores). The experimental results demonstrate that the integrated

system achieves high technical efficiency with Precision, Recall, and F1-scores of 1.0 (100%) and an average detection time of 5.31 seconds. Furthermore, the average Security Awareness Score increased significantly from 6.88 to 16.84, confirming that utilizing AI-interpreted alerts and systematic improvements via the PDCA cycle can effectively bridge the knowledge gap and enhance the cyber threat response efficiency of non-expert users. This research establishes a clear practical framework for integrating open-source tools to create real-time workflow automation suitable for small-scale organizations.

(Total 58 Pages)

Keywords: Cyber Threats, Detection System (Wazuh IDS + AI), Workflow Automation (n8n + PDCA)

_____ Advisor

กิตติกรรมประกาศ

การค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงอย่างสมบูรณ์ได้ด้วยความกรุณาอย่างยิ่งจาก ผู้ช่วยศาสตราจารย์ ดร.สุนันฑา สดสี อาจารย์ที่ปรึกษาที่ได้สละเวลาให้คำปรึกษา ชี้แนะแนวทาง และติดตามความคืบหน้าด้วยความเอาใจใส่เสมอมา ตลอดจนช่วยแก้ไขข้อบกพร่องต่างๆ จนงานวิจัยชิ้นนี้มีความสมบูรณ์ยิ่งขึ้น ผู้วิจัยขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ โอกาสนี้

ขอขอบคุณคณาจารย์ประจำสาขาวิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศทุกท่าน ที่ได้ถ่ายทอดความรู้ ประสบการณ์ และบ่มเพาะทักษะทางวิชาการอันเป็นรากฐานสำคัญที่ทำให้ผู้วิจัยสามารถดำเนินการค้นคว้าอิสระครั้งนี้ให้บรรลุวัตถุประสงค์ได้

ขอขอบคุณเพื่อนร่วมภาควิชาที่คอยแลกเปลี่ยนความคิดเห็นและให้ความช่วยเหลือด้วยดีเสมอมา จนทำให้การทำงานวิจัยชิ้นนี้สำเร็จเสร็จสิ้นลงได้

ท้ายที่สุดนี้ ผู้วิจัยหวังเป็นอย่างยิ่งว่าการค้นคว้าอิสระฉบับนี้จะเป็นประโยชน์และเป็นแนวทางในการต่อยอดเพื่อพัฒนาองค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ผู้ที่สนใจต่อไป

นัทธพงศ์ วิวิธสุรการ

สารบัญ

หน้า

บทคัดย่อภาษาไทย ..... ข
บทคัดย่อภาษาอังกฤษ ..... ง
กิตติกรรมประกาศ ..... ฉ
สารบัญ ..... ช
สารบัญตาราง ..... ฌ
สารบัญรูปภาพ ..... ญ
สารบัญรูปภาพ (ต่อ) ..... ฎ
บทที่ 1 บทนำ 1
1.1 ความเป็นมาและความสำคัญของปัญหา 1
1.2 วัตถุประสงค์ของการวิจัย 1
1.3 ขอบเขตของการวิจัย 2
1.4 ประโยชน์ที่คาดว่าจะได้รับ 2
1.5 นิยามศัพท์เฉพาะ/คำจำกัดความในงานวิจัย 3
บทที่ 2 แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง 2
2.1 แนวคิดการจัดการคุณภาพและวัฏจักร PDCA 2
2.2 แนวคิดและทฤษฎีระบบตรวจจับภัยคุกคาม (IDS/SIEM) 2
2.3 งานวิจัยที่เกี่ยวข้อง 7
บทที่ 3 วิธีการดำเนินการวิจัย 6
3.1 ระเบียบวิธีวิจัย 6
3.2 กรอบแนวความคิดของงานวิจัย 6
3.3 ประชากรและกลุ่มตัวอย่าง 11
3.4 เครื่องมือและอุปกรณ์ที่ใช้ในการวิจัย 12
3.5 เกณฑ์การวัดผลและการวิเคราะห์ข้อมูล 13
3.6 ขั้นตอนการดำเนินงานวิจัยตามวัฏจักร PDCA 21
3.7 มาตรการความปลอดภัยและแผนการรับมือ (Rollback) 41
3.8 แผนผังขั้นตอนการดำเนินงาน (Operation Plan) 42
บทที่ 4 ผลการวิจัยและอภิปรายผล 45
4.1 ผลการประเมินประสิทธิภาพด้านระบบ (System Metrics) 45

4.2 ผลการประเมินประสิทธิภาพด้านผู้ใช้งาน (User Metrics) 47
4.3 ผลการวิเคราะห์เชิงคุณภาพ (Qualitative Analysis) 51
4.4 อภิปรายผล 52
4.5 ข้อสรุป 53
บทที่ 5 สรุปผลการวิจัย และข้อจำกัด 54
5.1 สรุปผลการวิจัย 54
5.2 ข้อจำกัด และข้อเสนอแนะ 55
5.3 การเติมเต็มช่องว่างงานวิจัย 56
บรรณานุกรม 57
ประวัติผู้เขียน 58

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

สารบัญตาราง

ตารางที่		หน้า
2-1	งานวิจัยที่เกี่ยวข้อง	8
3-1	กรอบแนวคิดของงานวิจัย	10
3-2	วิธีการเก็บค่าและเป้าหมายความสำเร็จของกรณีที่ 1	14
3-3	วิธีการเก็บค่าและเป้าหมายความสำเร็จของกรณีที่ 2	15
3-4	รายละเอียดฐานข้อมูล Google Sheet สำหรับการโจมตีประเภท Phishing	19
3-5	รายละเอียดฐานข้อมูล Google Sheet สำหรับการโจมตีประเภท Bruteforce	20
3-6	มาตรการความปลอดภัยและแผนการรับมือ	41
3-7	แผนผังขั้นตอนการดำเนินงาน	43
4-1	ค่ารายการสถิติเวลาตอบสนองของผู้ใช้ Phishing	48
4-2	ค่ารายการสถิติเวลาตอบสนองของผู้ใช้ Bruteforce	48
4-3	ค่ารายการสถิติการตอบสนองที่ถูกต้องของผู้ใช้ Phishing	49
4-4	ค่ารายการสถิติการตอบสนองที่ถูกต้องของผู้ใช้ Bruteforce	50
4-5	ค่าสถิติความตระหนักรู้ด้านความปลอดภัยจากคะแนนแบบทดสอบ	51

พระจอมเกล้าพระนครเหนือ มหาวิทยาลัยเทคโนโลยี

สารบัญรูปภาพ

ภาพที่ หน้า

3-1 ผังการทำงานระบบแจ้งเตือน (System Workflow) 22
3-2 ตัวอย่างแบบทดสอบก่อน/หลังการทดลอง 24
3-3 คำสั่ง (Prompt) สำหรับแจ้งเตือนผู้ใช้หลังกดลิงก์ Phishing 25
3-4 คำสั่ง (Prompt) สำหรับเริ่มโจมตีผู้ใช้ด้วยวิธี Bruteforce 26
3-5 ตัวอย่างอีเมล Phishing จำลอง 27
3-6 หน้าเว็บจำลอง Phishing สำหรับอบรม 27
3-7 Workflow สำหรับรับจากแจ้งเตือนมาทำ Phishing 28
3-8 ตัวอย่างผลลัพธ์ข้อความแจ้งเตือนผู้ใช้ในการทำ Phishing 28
3-9 ระบบรายงานการถูกโจมตี (Report System) 29
3-10 Workflow n8n สำหรับบันทึกการเปลี่ยนรหัสผ่านของ Phishing 29
3-11 Workflow n8n สำหรับเริ่มการโจมตีจำลองของ Bruteforce 30
3-12 ผลลัพธ์ข้อความแจ้งเตือนผู้ใช้ในการจำลองการโจมตี Bruteforce 30
3-13 หน้าเปลี่ยนรหัสผ่านบนระบบรายงาน (Report System) 31
3-14 Workflow สำหรับบันทึกการเปลี่ยนรหัสผ่านของ Bruteforce 31
3-15 ไฟล์ ossec.conf บน Wazuh Agent ในเครื่องผู้ใช้ 32
3-16 เพิ่ม Sysmon ในไฟล์ ossec.conf บน Wazuh Agent ในเครื่องผู้ใช้ 33
3-17 ติดตั้ง Cloudflared ในเครื่องผู้ใช้ 33
3-18 ตั้งค่า Task schedule บนเครื่องผู้ใช้ 34
3-19 แก้ไขไฟล์ ossec.conf บน LinuxServer 35
3-20 แก้ไขไฟล์ local_rules.xml บน Wazuh Server 35
3-21 Workflow สำหรับรับการแจ้งเตือนเมื่อผู้ใช้กดลิงก์ Phishing 36
3-22 Workflow บันทึกเวลาการเปลี่ยนรหัสผ่านของ Phishing 36
3-23 Workflow สำหรับรับการแจ้งเตือนเมื่อผู้ใช้กดลิงก์ Phishing 37
3-24 Workflow สำหรับบันทึกการเปลี่ยนรหัสผ่านของ Bruteforce 37
3-25 ตัวอย่างวิดีโอการอบรม 38
3-26 คู่มือการตอบสนองต่อภัยคุกคาม 38
4-1 วัดผลกระทบของ Server ต่อทรัพยากรระบบในสถานการณ์ปกติ 46
4-2 วัดผลกระทบของ Agent ต่อทรัพยากรระบบในสถานการณ์ปกติ 46

สารบัญรูปภาพ (ต่อ)

ภาพที่ หน้า

4-3 วัดผลกระทบของ Server ต่อทรัพยากรระบบในสถานการณ์โหลดสูง 47

4-4 วัดผลกระทบของ Agent ต่อทรัพยากรระบบในสถานการณ์โหลดสูง 47

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันภัยคุกคามทางไซเบอร์มีความซับซ้อนและเพิ่มจำนวนขึ้นอย่างต่อเนื่องในขณะที่ระบบรักษาความปลอดภัย ระดับองค์กรส่วนใหญ่มักมีความซับซ้อนมีค่าใช้จ่ายสูงและต้องพึ่งพาผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์โดยตรง ทำให้ผู้ใช้งานทั่วไป เช่น ผู้ใช้ตามบ้านหรือองค์กรขนาดเล็กที่ไม่มีทีมด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์ไม่สามารถเข้าถึงหรือใช้งานระบบป้องกันภัยที่มีประสิทธิภาพได้

งานวิจัยนี้จึงมีความสำคัญในการตอบโจทย์ช่องว่างดังกล่าวมุ่งเน้นที่การพัฒนาระบบต้นแบบที่ใช้เครื่องมือ Open-Source (เช่น Wazuh IDS) ร่วมกับระบบ Automation อย่าง n8n และประดิษฐ์ (AI) เพื่อแปลงและสรุปผลการแจ้งเตือนภัยให้เข้าใจง่าย การบูรณาการนี้จะช่วยให้สามารถตรวจจับ ตอบสนอง และแจ้งเตือนภัยคุกคามได้แบบ Real-time และเป็นอัตโนมัติซึ่งช่วยลดการพึ่งพาผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์โดยตรง ทำให้ผู้ใช้งานทั่วไปสามารถเข้าใจและตอบสนองต่อภัยคุกคามได้อย่างถูกต้อง นอกจากนี้ ยังมีการนำวัฏจักร PDCA มาใช้เป็นกลไกหลักในการปรับปรุงระบบและพัฒนาความตระหนักรู้ด้านความปลอดภัย (Security Awareness) ของพนักงานอย่างต่อเนื่อง

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อพัฒนาและบูรณาการระบบต้นแบบสำหรับการตรวจจับภัยคุกคามไซเบอร์โดยใช้ Wazuh IDS ร่วมกับระบบ n8n และโมเดล AI ในการแปลผลและสรุปการแจ้งเตือน

1.2.2 เพื่อประเมินประสิทธิภาพของระบบที่พัฒนาขึ้นทั้งในด้านความแม่นยำในการตรวจจับและความสามารถในการตอบสนองของผู้ใช้

1.2.3 เพื่อปรับปรุงประสิทธิภาพการตอบสนองของผู้ใช้งานทั่วไปต่อภัยคุกคามไซเบอร์ผ่านการประยุกต์ใช้วัฏจักร PDCA

1.3 ขอบเขตของการวิจัย

1.3.1 การพัฒนาและบูรณาการระบบมุ่งเน้นการพัฒนาระบบต้นแบบด้วยเครื่องมือแบบ Open-Source (Wazuh IDS และ n8n) ที่เชื่อมต่อกับ AI เพื่อแปลผลและสรุปการแจ้งเตือนให้ผู้ใช้เข้าใจง่าย

1.3.2 กลุ่มเป้าหมายของการทดลองจำกัดเฉพาะกลุ่มพนักงาน/ผู้ใช้งานทั่วไป 25 คน

1.3.3 ระเบียบวิธีวิจัยดำเนินการภายใต้วัฏจักร PDCA (Plan, Do, Check, Act) เพื่อให้เกิดการปรับปรุงระบบและการสร้างความตระหนักรู้ด้านความปลอดภัยอย่างต่อเนื่อง

1.3.4 การวัดผลด้านเทคนิคเป็นการประเมินประสิทธิภาพทางเทคนิคของระบบ Wazuh ด้วยตัวชี้วัดหลัก ได้แก่ Precision, Recall, F1-score และ Detection Time

1.3.5 การวัดผลด้านผู้ใช้เป็นประเมินผลลัพธ์การปรับปรุงด้วยตัวชี้วัดหลัก ได้แก่ เวลาตอบสนองของผู้ใช้ อัตราการตอบสนองที่ถูกต้องและคะแนน Post-test

1.3.6 การวัดความตระหนักรู้ของผู้ใช้งานจะมีการทดสอบก่อนและหลังการวิจัยเพื่อวัดผลความตระหนักรู้ของผู้ใช้งาน

1.3.7 การโจมตีจำลองเป็นการโจมตีจำลองโดยผู้วิจัยเกี่ยวข้องกับผู้ใช้โดยตรงได้แก่ Phishing (ใช้เว็บจำลองสำหรับเก็บข้อมูลการคลิก) และ Bruteforce อย่างละ 125 ครั้ง

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 ประโยชน์ที่คาดว่าจะได้รับด้านผู้ใช้งานทั่วไปและองค์กร มีดังนี้

1.4.1.1 การลดความเสี่ยงและความซับซ้อนของผู้ใช้งานทั่วไปที่ไม่ใช่ผู้เชี่ยวชาญสามารถเข้าถึงและติดตั้งระบบรักษาความปลอดภัยไซเบอร์ระดับองค์กรได้ด้วยตนเองที่ในองค์กรขนาดเล็กมีค่าใช้จ่ายต่ำ (เนื่องจากใช้ Open-Source)

1.4.1.2 การเพิ่มประสิทธิภาพการตอบสนองสามารถลดเวลาตอบสนองของผู้ใช้ต่อภัยคุกคามและเพิ่มอัตราการตอบสนองที่ถูกต้องได้อย่างชัดเจนผ่านระบบแจ้งเตือนที่แปลผลด้วย AI

1.4.1.3 ผลลัพธ์จากการพัฒนาความตระหนักรู้โดยใช้ PDCA และการเปรียบเทียบผล Pre-test/Post-test จะช่วยยืนยันและวัดผลความตระหนักรู้ด้านความปลอดภัยของผู้ใช้ซึ่งสามารถนำไปปรับปรุง Training Program ได้อย่างมีประสิทธิภาพ

1.4.2 ประโยชน์ที่คาดว่าจะได้รับด้านวิชาการและเทคโนโลยี มีดังนี้

1.4.2.1 แนวทางปฏิบัติในการบูรณาการเริ่มต้นจากการสร้างระบบต้นแบบและแนวทางปฏิบัติ (Methodology) ที่ชัดเจนในการบูรณาการเครื่องมือ Wazuh IDS เข้ากับระบบ

Automation n8n และ AI เพื่อสร้าง เครื่องมือ Workflow Automation ที่มีประสิทธิภาพและเป็นอัตโนมัติแบบ Real-time

1.4.2.2 งานวิจัยนี้เติมเต็มช่องว่างที่งานวิจัยก่อนหน้ายังไม่ครอบคลุมโดยเน้นไปที่การประยุกต์ใช้ Automation และ AI ในการแปลผลการแจ้งเตือนและการประเมินผลลัพธ์จากมุมมองของผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญ (Non-expert Usability)

1.4.2.3 นำเสนอรูปแบบการนำวัฏจักร PDCA มาใช้เป็นกลไกขับเคลื่อนหลักในการปรับปรุงทั้งด้านเทคนิคของระบบและด้านความรู้ของบุคลากรในบริบทของการจัดการภัยคุกคามไซเบอร์อย่างต่อเนื่อง

1.5 นิยามศัพท์เฉพาะ/คำจำกัดความในงานวิจัย

1.5.1 PDCA (Plan-Do-Check-Act Cycle) หมายถึงกรอบการทำงานเพื่อการปรับปรุงอย่างต่อเนื่อง ซึ่งถูกนำมาใช้เป็นแนวทางหลักในงานวิจัยนี้เพื่อเพิ่มประสิทธิภาพการตรวจจับภัยคุกคามของระบบ Wazuh IDS และสร้างความตระหนักรู้ด้านความปลอดภัยให้แก่พนักงานในองค์กรอย่างเป็นระบบ

1.5.2 ระบบต้นแบบความปลอดภัยไซเบอร์ (Security Prototype System) หมายถึงระบบต้นแบบนี้สร้างขึ้นใหม่จากการนำเครื่องมือ Open-Source (Wazuh IDS และ n8n) มารวมเข้ากับปัญญาประดิษฐ์ (AI) โดยมีหน้าที่ให้ AI รับการแจ้งเตือนทางเทคนิคแล้วแปลผล สรุป และส่งข้อความแจ้งเตือนภัยคุกคามที่เข้าใจง่ายไปยังผู้ใช้งาน

1.5.3 Wazuh Intrusion Detection System (IDS) หมายถึงระบบตรวจจับการบุกรุกแบบ Open-Source ที่ถูกนำมาใช้ในงานวิจัยนี้เพื่อทำหน้าที่เก็บและวิเคราะห์บันทึกเหตุการณ์ของระบบ (Log) จากเครื่องลูกข่าย (Agents) ในรูปแบบต่างๆ

1.5.4 ระบบอัตโนมัติ (Automation System) หมายถึงการใช้เครื่องมือ n8n เป็น Workflow Engine ในการสร้าง Workflow อัตโนมัติเพื่อรับการแจ้งเตือนดิบ (Raw JSON) จาก Wazuh และดำเนินการส่งต่อการแจ้งเตือนไปยัง AI Model เพื่อประมวลผลก่อนที่จะแจ้งเตือนไปยังผู้ใช้งานปลายทางโดยไม่จำเป็นต้องมีผู้เชี่ยวชาญเข้ามาเกี่ยวข้อง

1.5.5 เวลาตอบสนองของผู้ใช้ (User Response Time) หมายถึงระยะเวลาที่ถูกบันทึกไว้ตั้งแต่ผู้ใช้งานได้รับข้อความแจ้งเตือนที่ถูกแปลผลโดย AI จนกระทั่งผู้ใช้งานได้ดำเนินการกระทำที่ถูกต้อง เพื่อตอบสนองต่อภัยคุกคามนั้นๆ ได้แก่ การรายงานที่เว็บไซต์ที่จัดเตรียมไว้หรือการเปลี่ยนรหัสผ่าน

1.5.6 ความตระหนักรู้ด้านความปลอดภัย (Security Awareness) หมายถึงระดับความรู้ความเข้าใจของผู้ใช้งานทั่วไปเกี่ยวกับประเภทของภัยคุกคาม ความหมายของการแจ้งเตือนและ

ขั้นตอนการตอบสนองที่ถูกต้องต่อภัยคุกคาม ซึ่งจะถูกวัดและประเมินผลด้วยแบบทดสอบ (Pre-test และ Post-test) ในขั้นตอนการตรวจสอบ (Check) ของวัฏจักร PDCA

1.5.7 ภัยคุกคามไซเบอร์จำลอง (Simulated Cybersecurity Threats) หมายถึงการโจมตีทางไซเบอร์ที่ถูกออกแบบและดำเนินการโดยผู้วิจัยเองได้แก่ การโจมตีแบบ Phishing และ Bruteforce โดยมีวัตถุประสงค์เพื่อจำลองสถานการณ์จริงเพื่อกระตุ้นให้ระบบ Wazuh สร้างการแจ้งเตือนและวัดผลการตอบสนองของผู้ใช้งานตามวัตถุประสงค์ของการวิจัย

1.5.8 Phishing (ฟิชชิง) หมายถึงการโจมตีจำลองในงานวิจัยนี้ โดยผู้วิจัยส่งอีเมลปลอมจำนวน 15 รูปแบบเพื่อหลอกล่อให้ผู้ใช้งานคลิกลิงก์ไปยังเว็บไซต์จำลองที่จัดเตรียมไว้ ซึ่งเป็นการวัดความสามารถของผู้ใช้ในการระบุและตอบสนองต่อการแจ้งเตือนภัยอย่างถูกต้อง

1.5.9 Bruteforce (การโจมตีแบบ Bruteforce) หมายถึงการโจมตีจำลองที่มุ่งเน้นการพยายามเข้าถึงบัญชีผู้ใช้ด้วยการสุ่มรหัสผ่านหลายครั้ง ซึ่งในงานวิจัยนี้เป็นการจำลองการแจ้งเตือนเพื่อวัดผลว่าผู้ใช้งานจะดำเนินการเปลี่ยนรหัสผ่านตามคำแนะนำภายในระยะเวลาที่กำหนดหรือไม่

1.5.10 เกณฑ์วัดผลด้านระบบ (System Metrics) หมายถึงชุดตัวชี้วัดทางสถิติที่ใช้ประเมินประสิทธิภาพทางเทคนิคของระบบตรวจจับภัยคุกคาม Wazuh IDS ได้แก่ Precision, Recall, และ F1-score ซึ่งเป็นค่าที่ใช้ยืนยันความแม่นยำและความสามารถในการตรวจจับภัยคุกคามได้ครบถ้วนของระบบที่พัฒนาขึ้น

1.5.11 ระบบรายงานการถูกโจมตี (Report System) หมายถึงระบบเว็บไซต์ที่ถูกสร้างขึ้นโดยผู้วิจัยเพื่อใช้เป็นเครื่องมือและช่องทางหลักให้ผู้ใช้งานใช้ในการดำเนินการตอบสนองที่ถูกต้องต่อภัยคุกคามจำลอง ตามคำแนะนำที่ได้รับจากการอบรมก่อนเริ่มการวิจัย

บทที่ 2
แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดการจัดการคุณภาพและวัฏจักร PDCA

วัฏจักร PDCA (Plan-Do-Check-Act Cycle) เป็นแนวคิดพื้นฐานด้านการจัดการคุณภาพและเป็นกรอบการทำงานที่ทรงพลังสำหรับการปรับปรุงอย่างต่อเนื่อง (Continuous Improvement) ตามแนวคิดของ (Deming, 1986) ซึ่งในงานวิจัยนี้ถูกนำมาใช้เป็นกรอบแนวคิดหลัก วัตถุประสงค์คือการเพิ่มประสิทธิภาพการตรวจจับภัยคุกคามและการสร้างความตระหนักรู้ด้านความปลอดภัย (Security Awareness) ในองค์กรอย่างเป็นระบบ โดยความสำคัญของ PDCA คือการบังคับให้เกิดการวัดผล (Check) และปรับปรุง (Act) อย่างเป็นวัฏจักร ซึ่งถือเป็นกลไกสำคัญในการรับมือกับภัยคุกคามไซเบอร์ที่มีการเปลี่ยนแปลงและพัฒนาอยู่ตลอดเวลา

2.2 แนวคิดและทฤษฎีระบบตรวจจับภัยคุกคาม (IDS/SIEM)

ระบบตรวจจับภัยคุกคาม (Intrusion Detection System: IDS) และระบบจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Information and Event Management: SIEM) เป็นรากฐานสำคัญของการจัดการภัยคุกคามไซเบอร์ระดับองค์กร โดยระบบ IDS ในปัจจุบันมักใช้การผสมผสานหลายทฤษฎีเข้าด้วยกันเพื่อเพิ่มประสิทธิภาพในการตรวจจับ ตัวอย่างเช่น Wazuh IDS ที่ถูกนำมาใช้ในงานวิจัยนี้เป็นระบบ SIEM แบบ Open-Source ที่ใช้หลักการทำงานร่วมกันตามทฤษฎีดังนี้

2.2.1 ทฤษฎีการตรวจจับการบุกรุกแบบลายเซ็น (Signature-based Detection) ถือเป็นแนวคิดพื้นฐานและเป็นที่ยอมรับอย่างกว้างขวางในระบบตรวจจับภัยคุกคาม (IDS) โดยหลักการทำงานสำคัญคือการอ้างอิงจากลายเซ็นดิจิทัล (Digital Signatures) ที่เป็นเอกลักษณ์ของรูปแบบหรือลำดับของการโจมตีทางไซเบอร์ที่เป็นที่รู้จักแล้ว ลายเซ็นเหล่านี้จะถูกจัดเก็บไว้ในฐานข้อมูลขนาดใหญ่ของระบบ IDS ซึ่งเมื่อเกิดกิจกรรมใดๆ ขึ้นในระบบ ไม่ว่าจะเป็นข้อมูลในแพ็กเก็ตเครือข่ายหรือบันทึกเหตุการณ์ของระบบ (Log) ตัวระบบจะทำการเปรียบเทียบกิจกรรมที่เกิดขึ้นแบบทันท่วงทีกับลายเซ็นที่ถูกกำหนดไว้ล่วงหน้า หากกิจกรรมใดๆ ตรงกับลายเซ็นที่กำหนดไว้ก็จะถือว่ากิจกรรมนั้นเป็นการโจมตี (Anderson, 1980) วิธีนี้มีข้อดีที่โดดเด่นคือการให้ผลลัพธ์ที่มีความแม่นยำสูง (High Accuracy) และมีความแน่นอนในการระบุภัยคุกคามที่เคยเกิดขึ้นและมีการบันทึกรูปแบบไว้แล้ว

อย่างไรก็ตาม จุดอ่อนสำคัญของ Signature-based Detection คือการต้องพึ่งพาฐานข้อมูลลายเซ็นที่ได้รับการปรับปรุงอย่างต่อเนื่องและจะไม่สามารถตรวจจับการโจมตีใหม่ (Zero-day Attacks) ที่ยังไม่มีลายเซ็นถูกสร้างหรืออัปเดตลงในฐานข้อมูลของระบบได้ ด้วยข้อจำกัดนี้เองทำให้ระบบ IDS ในปัจจุบัน เช่น Wazuh IDS มักใช้ทฤษฎีนี้ร่วมกับการตรวจจับความผิดปกติ (Anomaly Detection Theory) เพื่อเติมเต็มช่องว่างในการรับมือกับภัยคุกคามที่ไม่เคยพบมาก่อน

2.2.2 ทฤษฎีการตรวจจับความผิดปกติ (Anomaly Detection Theory) ที่เสนอโดย (Denning, 1987) มีรูปแบบการทำงานที่มุ่งเน้นการสร้าง "แบบแผนปกติ" (Baseline) จากพฤติกรรมปกติของผู้ใช้งานหรือระบบอย่างต่อเนื่อง จากนั้นระบบจะเฝ้าสังเกตและตรวจจับพฤติกรรมที่ “แตกต่างไปจากแบบแผนปกติ” ที่กำหนดไว้อย่างต่อเนื่อง ซึ่งเป็นหลักการพื้นฐานที่แตกต่างจากการค้นหาลายเซ็นการโจมตีที่รู้จักตามแนวคิด Signature-based detection สำหรับวิธีการดำเนินงานหลักเพื่อสร้างและประเมินแบบแผนปกตินี้ จะอาศัยการประยุกต์ใช้หลักการทางสถิติ (Statistical-based) เพื่อคำนวณเมตริกความถี่และขอบเขตของการดำเนินการและการเรียนรู้ของเครื่องจักร (Machine Learning) ในการวิเคราะห์บันทึกเหตุการณ์ของระบบหรือกิจกรรมเครือข่าย เพื่อให้สามารถระบุและจำแนกรูปแบบพฤติกรรมที่ไม่คาดคิดหรือแตกต่างจากเดิมได้อย่างละเอียด ส่วนในกระบวนการการทำงานนั้นคือ การระบุกิจกรรมที่อาจเป็นการบุกรุกเมื่อพฤติกรรมของผู้ใช้หรือระบบเบี่ยงเบน ไปจากแบบแผนปกติที่สร้างไว้ โดยมีข้อได้เปรียบที่สำคัญที่สุดคือความสามารถในการตรวจจับหมายถึงที่ไม่เคยพบมาก่อน (Zero-day attacks) อันเป็นการช่วยเติมเต็มจุดอ่อนของวิธีการตรวจจับแบบ Signature-based detection

อย่างไรก็ตาม ข้อจำกัดโดยธรรมชาติของวิธี Anomaly Detection คือการต้องพึ่งพาความแม่นยำของชุดข้อมูลที่ใช้ในการกำหนดแบบแผนปกติอย่างสูง เนื่องจากหากแบบแผนปกติไม่สมบูรณ์หรือไม่ได้รับการปรับปรุงอย่างต่อเนื่อง จะส่งผลให้เกิดความซับซ้อนในการแยกแยะระหว่างความผิดปกติที่เป็นการบุกรุกจริงกับกิจกรรมใหม่ๆ ที่ถูกต้องตามกฎหมายของระบบ ซึ่งอาจนำไปสู่อัตราการแจ้งเตือนที่ผิดพลาด (False Positives) ที่สูงและทำให้ผู้ดูแลระบบสับสนได้

2.2.3 แนวคิดระบบอัตโนมัติ (Automation) และการประยุกต์ใช้ AI ใน Cybersecurity ได้เข้ามามีบทบาทสำคัญในการรับมือกับความซับซ้อนของภัยคุกคามทางไซเบอร์ที่มีจำนวนเพิ่มขึ้นอย่างต่อเนื่อง โดยระบบอัตโนมัติทำหน้าที่เป็น Workflow เพื่อเชื่อมโยงเครื่องมือด้านความปลอดภัยที่แตกต่างกันเข้าด้วยกันให้สามารถทำงานได้อย่างรวดเร็วและต่อเนื่องโดยไม่จำเป็นต้องใช้มนุษย์ ซึ่งแนวคิดนี้ได้รับการสนับสนุนจากงานวิจัยของ (Seara & Serrão, 2024) ที่เสนอระบบสแกนช่องโหว่ความปลอดภัยแบบอัตโนมัติด้วยซอฟต์แวร์ Open-Source สำหรับผู้ใช้ทั่วไป รูปแบบของระบบนี้คือการใช้เครื่องมือ Workflow Engine แบบ Open-Source อย่าง n8n ในการสร้าง Workflow

Automation แบบทันท่วงที (Real-time) ที่บูรณาการเข้ากับระบบตรวจจับภัยคุกคาม (Wazuh IDS) และปัญญาประดิษฐ์ (AI/LLM) เพื่อให้ระบบสามารถทำงานได้มีประสิทธิภาพมากขึ้น

ในงานวิจัยนี้ระบบอัตโนมัติ n8n ถูกนำมาใช้ในการสร้างเครื่องมือ Workflow Automation แบบทันท่วงทีโดยมีบทบาทหลักสามส่วนคือ การรับการแจ้งเตือนจาก IDS โดยทำหน้าที่รับข้อมูลการแจ้งเตือนดิบ (Raw JSON) ที่ส่งมาจาก Wazuh Server ผ่าน Webhook ตามมาด้วยการส่งต่อข้อมูลและการประมวลผล ซึ่งจะส่งต่อการแจ้งเตือนดิบไปยังโมเดลปัญญาประดิษฐ์ใน n8n Workflow เพื่อให้ AI ดำเนินการแปลผลให้เป็นภาษาที่เข้าใจง่ายและส่วนสุดท้ายคือการแจ้งเตือนปลายทาง ซึ่งจะส่งต่อผลลัพธ์การแปลผลที่กระชับและเข้าใจง่ายไปยังช่องทางสื่อสารของผู้ใช้งาน (Telegram)

ส่วนสำคัญของการบูรณาการคือการประยุกต์ใช้ปัญญาประดิษฐ์และโมเดลภาษาขนาดใหญ่ โดยมีวัตถุประสงค์เพื่อแก้ไขช่องว่างด้านความเชี่ยวชาญของผู้ดูแลระบบที่งานวิจัยก่อนหน้ายังไม่ได้ครอบคลุม โดยโมเดล AI ทำหน้าที่เป็นล่ามแปลศัพท์เทคนิคด้าน Cybersecurity ที่ซับซ้อนและเข้าใจยากในการแจ้งเตือนของ Wazuh ให้เป็น ข้อความแจ้งเตือนที่ชัดเจนและกระชับเพื่อลดความสับสนของผู้ใช้งานทั่วไป รวมไปถึงคำแนะนำที่ต้องดำเนินการทันทีเพื่อช่วยให้ผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญสามารถตอบสนองต่อภัยคุกคามได้อย่างถูกต้องตามขั้นตอนและภายในระยะเวลาที่กำหนด

การบูรณาการระบบอัตโนมัติ ควบคู่ไปกับปัญญาประดิษฐ์นี้จึงเป็นกลไกสำคัญที่ช่วยลดการพึ่งพาผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์โดยตรงและเพิ่มประสิทธิภาพในการตอบสนองต่อภัยคุกคามไซเบอร์ของผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญได้อย่างชัดเจน

2.3 งานวิจัยที่เกี่ยวข้อง

การทบทวนงานวิจัยที่เกี่ยวข้อง แสดงดังตารางที่ 2-1 ชี้ให้เห็นว่าการประยุกต์ใช้ระบบตรวจจับการบุกรุก SIEM แบบ Open-Source เช่น Wazuh เริ่มเป็นที่แพร่หลายในเครือข่ายองค์กรและสถาบันการศึกษา (Gbedawo et al., 2017) และมีการพัฒนาเทคนิคในด้านความแม่นยำในการตรวจจับอย่างต่อเนื่อง ด้วย Machine Learning (Chamkar et al., 2023) อย่างไรก็ตามงานวิจัยส่วนใหญ่มักมุ่งเน้นไปที่ การแก้ไขปัญหาและปรับปรุงประสิทธิภาพในมิติทางเทคนิค (Detection Accuracy) หรือการ เปรียบเทียบประสิทธิภาพระดับองค์กร (Manzoor et al., 2024) แต่ยังขาดการศึกษาในมิติของ ‘ผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์’

ตารางที่ 2-1 งานวิจัยที่เกี่ยวข้อง

ผู้วิจัยและปี	ชื่อบทความ	สาระสำคัญ/ผลงาน	ช่องว่าง
(Gbedawo, Sedegah, & Mensah, 2017)	Intrusion detection on campus network, the open-source approach Accra Technical University case study	เป็นการนำแนวคิดของ IDS และเครื่องมือแบบ Open-Source มาใช้ในการตรวจจับการบุกรุกในมหาวิทยาลัย	เป็นการใช้งานในเครือข่ายองค์กร/มหาวิทยาลัยยังขาดการประยุกต์ใช้สำหรับผู้ใช้งานทั่วไป
(Chamkar, Nawari, & Singh, 2023)	Improving threat detection in Wazuh using machine learning techniques	มุ่งเน้นการปรับปรุงประสิทธิภาพการตรวจจับภัยคุกคามในระบบ Wazuh IDS โดยใช้เทคนิคของ Machine Learning (ML)	เน้นการปรับปรุงด้านเทคนิค (Detection Accuracy) แต่ไม่ได้ครอบคลุม การเชื่อมต่อกับ ระบบอัตโนมัติเพื่อแปลผลให้ผู้ใช้เข้าใจง่าย
(Manzoor et al., 2024)	Evaluating Security and Performance of Open-Source SIEM Solutions for SMEs	ประเมินและเปรียบเทียบประสิทธิภาพของ SIEM แบบ Open-Source หลายตัว ซึ่งรวมถึง Wazuh สำหรับองค์กรขนาดเล็กแบบ SMEs	ไม่ได้เจาะลึกการสร้าง Automation Pipeline หรือการใช้ AI ในการแจ้งเตือนอัตโนมัติไปยังผู้ใช้งานโดยตรง
(Seara & Serrão , 2024)	Automation of System Security Vulnerabilities Detection Using Open-Source Software	เสนอระบบสแกนช่องโหว่แบบ อัตโนมัติด้วย Open-Source สำหรับผู้ใช้ทั่วไป	ระบบเน้นการสแกนช่องโหว่สำหรับผู้ใช้ทั่วไปแต่ยังไม่ครอบคลุมการตอบสนองเชิงลึกแบบทันท่วงทีไปยังผู้ใช้

จากการทบทวนงานวิจัยที่เกี่ยวข้องของตารางที่ 2-1 ผู้วิจัยจึงกำหนดให้งานวิจัยนี้จึงมุ่งเน้นการเติมเต็มช่องว่างดังกล่าว โดยการสร้างระบบบูรณาการ ที่ใช้ระบบอัตโนมัติควบคู่ไปกับปัญญาประดิษฐ์ในการแปลผลการแจ้งเตือนทางเทคนิค ให้เป็นข้อความแจ้งเตือนที่เข้าใจง่าย ซึ่งเป็นสิ่งที่งานวิจัยก่อนหน้ายังไม่ครอบคลุม นอกจากนี้ยังนำ เสนอรูปแบบการประยุกต์ใช้วัฏจักร PDCA เป็นกลไกขับเคลื่อนหลักในการปรับปรุงประสิทธิภาพการตอบสนองและความตระหนักรู้ด้านความปลอดภัยของผู้ใช้งานอย่างเป็นระบบและต่อเนื่อง

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

บทที่ 3
วิธีการดำเนินการวิจัย

3.1 ระเบียบวิธีวิจัย

งานวิจัยนี้ใช้วิธีการวิจัยเชิงปฏิบัติการ (Action Research) โดยมี PDCA เป็นกรอบการดำเนินงานหลักในการปรับปรุงอย่างต่อเนื่อง (Continuous Improvement) เพื่อให้เกิดการปรับปรุงประสิทธิภาพของระบบตรวจจับภัยคุกคามและการตอบสนองของผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์

3.2 กรอบแนวความคิดของงานวิจัย

กรอบแนวคิดนี้อธิบายถึงความสัมพันธ์ระหว่างองค์ประกอบหลัก 3 ส่วน ได้แก่ ตัวแปรต้น ตัวแปรแทรกซ้อนและตัวแปรตาม โดยมีวัตถุประสงค์เพื่อเพิ่มประสิทธิภาพการตอบสนองต่อภัยคุกคามไซเบอร์ของผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์ แสดงดังตารางที่ 3-1

ตารางที่ 3-1 กรอบแนวคิดของงานวิจัย

ตัวแปรต้น (Independent Variables)	ระบบบูรณาการ Wazuh/n8n/AI เริ่มตั้งแต่การติดตั้งและใช้งานระบบต้นแบบที่รวมเอา Wazuh IDS เข้ากับระบบ n8n และ AI เพื่อสร้างข้อความแจ้งเตือนที่เข้าใจง่ายสำหรับผู้ใช้
ตัวแปรแทรกซ้อน (Moderating Variable)	วัฏจักร PDCA ทำหน้าที่เป็นกรอบการดำเนินงานวิจัย เพื่อใช้ผลลัพธ์จากขั้นตอน Check ในการปรับปรุง Plan/Do อย่างต่อเนื่อง
ตัวแปรตาม (Dependent Variables)	ประสิทธิภาพการตอบสนองของผู้ใช้ (User Response Efficiency) วัดผลจากการลดลงของ ตัวแปรตาม (Dependent Variables) ประสิทธิภาพการตอบสนองของผู้ใช้

จากตารางที่ 3-1 แสดงถึงกรอบแนวคิดหลักของงานวิจัย โดยอธิบายความสัมพันธ์ระหว่างองค์ประกอบ 3 ส่วน คือ ตัวแปรต้น ซึ่งได้แก่ระบบบูรณาการ Wazuh/ n8n/AI ที่ทำหน้าที่สร้างข้อความแจ้งเตือนที่เข้าใจง่าย ตัวแปรแทรกซ้อน (Moderating Variable) คือ PDCA ที่เป็นกรอบการดำเนินงานหลักในการปรับปรุงอย่างต่อเนื่อง และตัวแปรตามคือประสิทธิภาพการตอบสนองของผู้ใช้ (User Response Efficiency) ซึ่งวัดผลจากการลดลงของเวลาตอบสนอง การเพิ่มขึ้นของอัตราตอบสนองที่ถูกต้องและคะแนน Post-test โดยมีวัตถุประสงค์เพื่อเพิ่มประสิทธิภาพการตอบสนองต่อภัยคุกคามไซเบอร์ของผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์

นอกจากนี้ จากการวิเคราะห์ตารางที่ 3-1 ดังกล่าว สามารถอธิบายความสัมพันธ์ของการเปลี่ยนแปลงและไม่เปลี่ยนแปลงของตัวแปรต้นกับตัวแปรอื่น ๆ ได้ดังนี้

ก) ถ้าตัวแปรต้นซึ่งคือ ระบบบูรณาการ Wazuh/n8n/AI ที่ทำหน้าที่สร้างข้อความแจ้งเตือนที่เข้าใจง่าย มีการเปลี่ยนแปลงหรือปรับปรุง เช่น ทำให้ข้อความ AI กระชับขึ้น หรือทำให้ระบบตอบสนองต่อการกระทำของผู้ใช้ได้เร็วขึ้น การเปลี่ยนแปลงนั้นจะถูกนำไปทดลองและประเมินผลภายใต้วัฏจักร PDCA (Plan-Do-Check-Act) เพื่อดูผลลัพธ์ เพื่อทำให้ตัวแปรตามอย่างการตอบสนองของผู้ใช้ดีขึ้น เช่น ผู้ใช้ใช้เวลาในการเปลี่ยนรหัสผ่านน้อยลง และมีอัตราการตอบสนองที่ถูกต้องสูงขึ้น

ข) ถ้าตัวแปรต้นไม่เปลี่ยนแปลง แต่ระบบการดำเนินงานยังคงอยู่ภายใต้การควบคุมของตัวแปรแทรกซ้อน ซึ่งคือ วัฏจักร PDCA วัฏจักรดังกล่าวจะใช้ผลลัพธ์จากการวัดผลในขั้นตอน Check เพื่อประเมินตัวแปรตาม ซึ่งก็คือ ประสิทธิภาพการตอบสนองของผู้ใช้ (User Response Efficiency) ว่ายังคงเป็นไปตามวัตถุประสงค์ของการวิจัยหรือไม่ โดยมุ่งเน้นการวัดผลจากการลดลงของเวลาตอบสนองการเพิ่มขึ้นของอัตราตอบสนองที่ถูกต้อง และคะแนน Post-test

3.3 ประชากรและกลุ่มตัวอย่าง

3.3.1 ประชากร (Population) ที่ใช้ในการวิจัยนี้คือพนักงานทั่วไปที่ไม่ใช่ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์ ซึ่งเป็นกลุ่มเป้าหมายที่งานวิจัยต้องการวัดผลและปรับปรุงประสิทธิภาพการตอบสนองต่อภัยคุกคามไซเบอร์

3.3.2 กลุ่มตัวอย่าง (Sample) ที่ใช้ในการวิจัยนี้คือพนักงานทั่วไปในองค์กรขนาดเล็กที่ไม่มีผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์จำนวนรวมทั้งสิ้น 25 คน โดยคุณสมบัติของกลุ่มตัวอย่างนี้ถูกกำหนดขึ้นอย่างชัดเจนเพื่อตอบวัตถุประสงค์หลักของงานวิจัย

3.3.2.1 ประการแรกคือ เป็นผู้ใช้งานคอมพิวเตอร์และอินเทอร์เน็ตในการทำงานประจำวันเพื่อให้มั่นใจว่าผู้เข้าร่วมการวิจัยจะได้รับภัยคุกคามไซเบอร์จำลองที่เกี่ยวข้องกับสถานการณ์การทำงานจริงและสามารถตอบสนองได้อย่างถูกต้อง

3.3.2.2 ประการที่สองคือ เป็นกลุ่มผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์ ซึ่งเป็นคุณสมบัติที่สำคัญที่สุด เนื่องจากวัตถุประสงค์หลักของโครงการนี้คือการเพิ่มประสิทธิภาพการตอบสนองต่อภัยคุกคามของผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์

3.3.2.3 ประการสุดท้ายคือ การยินยอมเข้าร่วมการวิจัยและได้รับการติดตั้ง Wazuh Agent บนเครื่องคอมพิวเตอร์ที่ใช้งาน ซึ่งเป็นข้อกำหนดทางเทคนิคที่จำเป็นต่อการวิจัย เชิงปฏิบัติการ เนื่องจาก Agent นี้เป็นเครื่องมือที่ใช้ในการเก็บและวิเคราะห์บันทึกเหตุการณ์ของ ระบบ เพื่อบันทึกพฤติกรรมการตอบสนองของผู้ใช้งาน และนำไปคำนวณ ซึ่งเป็นตัวชี้วัดสำคัญ ของงานวิจัย

3.4 เครื่องมือและอุปกรณ์ที่ใช้ในการวิจัย

3.4.1 ระบบตรวจจับภัยคุกคาม Wazuh Intrusion Detection System (Wazuh IDS) ซึ่งประกอบด้วย Wazuh Agent บนเครื่องลูกข่ายสำหรับการเก็บบันทึกเหตุการณ์ของระบบบนเครื่องผู้ใช้และส่งไปยัง Wazuh Server บนเครื่อง Server ซึ่งมีความจำเป็นในงานวิจัยนี้เนื่องจากทำหน้าที่เป็นระบบจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัย (SIEM) ที่ใช้เก็บบันทึกเหตุการณ์ของระบบของการโจมตีจำลองแบบ Phishing และ Bruteforce จากเครื่องผู้ใช้ไว้ทั้งหมด

3.4.2 ระบบอัตโนมัติและเครื่องมือ Workflow Automation n8n ถูกใช้เป็นเครื่องมือในการสร้าง Workflow เพื่อแก้ไขช่องว่างที่งานวิจัยก่อนหน้ายังไม่ครอบคลุม ทำให้สามารถตรวจจับตอบสนองและแจ้งเตือนภัยได้อย่างอัตโนมัติ นอกจากนี้ยังทำหน้าที่เป็นตัวกลางในการรับการแจ้งเตือนดิบ (Raw JSON) จาก Wazuh Server และส่งการแจ้งเตือนดิบดังกล่าวไปยังโมเดลปัญญาประดิษฐ์ที่อยู่ใน Workflow เพื่อให้ปัญญาประดิษฐ์ทำหน้าที่เป็น "ล่าม" ในการสรุปการแจ้งเตือนภัยให้เป็นภาษาที่เข้าใจง่ายและไม่ซ้ำกันในแต่ละครั้ง ก่อนจะส่งข้อความแจ้งเตือนที่แปลผลแล้วไปยังผู้ใช้งานปลายทางผ่าน Telegram ซึ่งช่วยลดการพึ่งพาผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์ในการแปลภาษาการแจ้งเตือนให้เป็นภาษาที่เข้าใจง่ายโดยตรง

3.4.3 ปัญญาประดิษฐ์และโมเดลภาษาขนาดใหญ่ทำหน้าที่เป็น "ล่าม" ในงานวิจัยนี้ ซึ่งเป็นสิ่งจำเป็นเพื่อแก้ไขช่องว่างระหว่างผู้ใช้งานทั่วไปกับผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์ให้แคบลง โดยเฉพาะอย่างยิ่งในการประยุกต์ใช้กับโครงการค้นคว้าอิสระนี้ เนื่องจากปัญญาประดิษฐ์จะรับการแจ้งเตือนทางเทคนิคที่ซับซ้อนจาก Wazuh Server มาแปลผลและสรุปคำแนะนำในการแก้ไขปัญหาเป็นข้อความแจ้งเตือนที่เป็นภาษามนุษย์ที่เข้าใจง่ายแก่ผู้ใช้งานผ่าน Telegram ด้วยเหตุผลสำคัญคือเพื่อให้ผู้ใช้สามารถตอบสนองต่อภัยคุกคามได้อย่างรวดเร็ว

และถูกต้อง อันเป็นกลไกสำคัญในการเพิ่มประสิทธิภาพการตอบสนองของผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์ตามวัตถุประสงค์ของการวิจัย

3.4.4 ระบบจัดเก็บและวัดผลข้อมูล (Google Sheet/Report System) ในงานวิจัยระบบนี้มีการประยุกต์ใช้ผ่านเครื่องมือหลักสองส่วน คือ Google Sheet ซึ่งใช้สำหรับจัดเก็บข้อมูลดิบเพื่อนำไปคำนวณค่าตัวชี้วัดด้านผู้ใช้งานและด้านระบบของการโจมตีจำลองทั้งแบบ Phishing และ Bruteforce ส่วนที่สองคือระบบรายงานการถูกโจมตี ซึ่งเป็นระบบเว็บไซต์ที่สร้างขึ้นเพื่อให้ผู้ใช้ใช้เป็นช่องทางในการเปลี่ยนรหัสผ่านตามคำแนะนำที่ผู้วิจัยแจ้งไว้ตอนอบรมก่อนเริ่มการวิจัย

3.5 เกณฑ์การวัดผลและการวิเคราะห์ข้อมูล

เกณฑ์การวัดผลของงานวิจัย แบ่งออกเป็น 2 ด้านหลักได้แก่ เกณฑ์วัดผลด้านผู้ใช้งาน (User Metrics) และด้านระบบ (System Metrics)

3.5.1 เกณฑ์วัดผลด้านผู้ใช้งานเป็นหัวใจสำคัญของการวิจัยเพื่อยืนยันว่าการบูรณาการระบบอัตโนมัติและปัญญาประดิษฐ์ (n8n/AI) สามารถช่วยให้ผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์ตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพจริง

3.5.1.1 เวลาตอบสนองของผู้ใช้ (User Response Time) หมายถึงระยะเวลาตั้งแต่ผู้ใช้ได้รับการแจ้งเตือนจนถึงขั้นตอนการดำเนินการเสร็จสิ้น เช่น หากได้รับการแจ้งเตือนจากการโจมตีแบบ Bruteforce และผู้ใช้ทำการเปลี่ยนรหัสผ่านซึ่งใช้เวลา 30 วินาที นับจากได้รับการแจ้งเตือนแสดงว่าเวลาตอบสนองของผู้ใช้เป็น 30 วินาที เป็นต้น การคำนวณค่าดังกล่าวมีความสำคัญเพื่อ ยืนยันว่าผู้ใช้มีความตระหนักรู้ด้านความปลอดภัย (Security Awearness) สามารถตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและถูกต้องตามวัตถุประสงค์ของการวิจัย

3.5.1.1.1 วิธีการวัดผลสำหรับการโจมตีจำลองแบบ Phishing แบ่งออกเป็น 2 กรณีได้แก่ ผู้ใช้เผลอกดลิงก์ Phishing และผู้ใช้ไม่ได้กดลิงก์ Phishing

ก) กรณีที่ 1 การคำนวณเวลาตอบสนองของผู้ใช้ (User Response Time) สำหรับกรณีที่ผู้ใช้เผลอกดลิงก์ Phishing นั้นจะมีวิธีการคำนวณแสดงดังสมการที่ 3-1

$$T_{Response} = T_{Acknowledge} - T_{Click} \tag{3-1}$$

เมื่อ $T_{Response}$ คือ เวลาตอบสนองของผู้ใช้

$T_{Acknowledge}$ คือ เวลาที่ผู้ใช้กดเปลี่ยนรหัสผ่านที่ระบบรายงาน

T_{Click} คือ เวลาที่ผู้ใช้เผลอกดลิงก์ Phishing บนอีเมล

จากสมการที่ 3-1 สามารถอธิบายได้ว่า ระยะเวลาตอบสนองนี้ถูกคำนวณจากความแตกต่างระหว่างเวลาที่ผู้ใช้งานได้ดำเนินการแก้ไขที่ถูกต้องในระบบรายงานการถูกโจมตี (Report System) ลบออกด้วย เวลาที่เกิดเหตุการณ์แรกขึ้น ซึ่งคือเวลาที่ผู้ใช้เผลอกดลิงก์ Phishing บนอีเมล

เนื่องจากผู้วิจัยต้องการประเมินความสามารถของผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์ว่าสามารถดำเนินการได้ทันเวลาและถูกต้องตามคำแนะนำหลังจากเผลอกดลิงก์ Phishing หรือไม่ ซึ่งผู้วิจัยได้ใช้วิธีการเก็บค่าและการตั้งเป้าหมายความสำเร็จแสดงดังตารางที่ 3-2 ซึ่งแสดงถึงวิธีการเก็บค่าและแหล่งที่มาของข้อมูลที่ใช้ในการคำนวณเวลาตอบสนองของผู้ใช้ โดยมีรายละเอียดคือ การเก็บเวลาที่ผู้ใช้กดลิงก์ Phishing บนอีเมลและเวลาที่ผู้ใช้กดเปลี่ยนรหัสผ่านบนระบบรายงานการถูกโจมตี ข้อมูลเหล่านี้มีแหล่งที่มาจากบันทึก เหตุการณ์ของระบบใน Wazuh Agent บนเครื่องผู้ใช้ ซึ่งมีเป้า หมายความสำเร็จที่ชัดเจนคือผู้ใช้ต้องสามารถกดเปลี่ยนรหัสผ่านได้ภายใน 90 วินาที หลังจากที่ผู้ใช้ เผลอกดลิงก์ Phishing บนอีเมลเพื่อประเมินความสามารถในการดำเนินการตอบสนองที่ถูกต้องและทันเวลาของผู้ใช้

ตารางที่ 3-2 วิธีการเก็บค่าและเป้าหมายความสำเร็จของกรณีที่ 1

สิ่งที่เก็บ	แหล่งที่มา
เวลาที่ผู้ใช้กดลิงก์ Phishing บนอีเมล	บันทึกเหตุการณ์ของระบบ Wazuh Agent
เวลาที่ผู้ใช้กดเปลี่ยนรหัสผ่านบนระบบรายงานการถูกโจมตี (Report System)	บันทึกเหตุการณ์ของระบบ Wazuh Agent โดยมีเป้าหมายความสำเร็จคือเปลี่ยนรหัสผ่านภายใน 90 วินาที หลังจากที่ผู้ใช้กดลิงก์ Phishing บนอีเมล

ข) กรณีที่ 2 เวลาตอบสนองของผู้ใช้ (User Response Time) สำหรับผู้ใช้ที่ไม่ได้คลิกลิงก์ Phishing ภายในระยะเวลาที่กำหนด (มากกว่า 7 วัน) มีวิธีการคำนวณแสดงดังสมการที่ 3-2

$$D_{Time} = T_{Check} - T_{Sent} \tag{3-2}$$

เมื่อ D_{Time} คือ ระยะเวลาที่ผ่านไป (เป็นวัน)

T_{Check} คือ เวลาที่ผู้วิจัยตรวจสอบและบันทึกสถานะ

T_{Sent} คือ เวลาที่ผู้วิจัยส่งอีเมล Phishing ออกไป

จากสมการที่ 3-2 ผู้วิจัยจะนำผลลัพธ์จากการคำนวณดังกล่าวมาตรวจสอบ กับสมการที่ 3-3 โดยสมการนี้ใช้เพื่อกำหนดว่าการดำเนินการนั้น ถูกต้อง (Correct) หรือไม่ เมื่อเปรียบเทียบกับเกณฑ์ 7 วัน และสถานะการไม่คลิกลิงก์ของผู้ใช้ (Did not Click) แสดงดังสมการที่ 3-3

$$R_{Correct} = (D_{Time} > 7)\ AND\ (U_{Status}\ is\ "Did\ not\ Click") \quad (3\text{-}3)$$

เมื่อ $R_{Correct}$ คือ สถานะผลลัพธ์ว่าถูกต้อง (Correct)

D_{Time} คือ ระยะเวลาที่ผ่านไป (เป็นวัน)

U_{Status} คือ สถานะการคลิกลิงก์ของผู้ใช้

เนื่องจากผู้วิจัยต้องการประเมินความตระหนักรู้ด้านความปลอดภัย (Security Awareness) ของผู้ใช้งานในการเพิกเฉยต่ออีเมลที่น่าสงสัยได้อย่างถูกต้อง การคำนวณในกรณีนี้จึงไม่ได้วัดจากความเร็วในการตอบสนองเป็นวินาทีแต่เป็นการวัดผลลัพธ์ว่าผู้ใช้สามารถหลีกเลี่ยงการกระทำที่ไม่ถูกต้องได้หรือไม่ ซึ่งผู้วิจัยได้ใช้วิธีการเก็บค่าเวลาที่ผู้วิจัยส่งอีเมล Phishing จำลองและสถานะการไม่ตอบสนองต่อลิงก์ Phishing ภายใน 7 วัน แสดงดังตารางที่ 3-3

ตารางที่ 3-3 แสดงถึงข้อมูลที่จัดเก็บประกอบด้วยสองช่วงเวลาหลักที่บันทึกโดยผู้วิจัย ช่วงแรกคือการเก็บเวลาที่ผู้วิจัยส่งอีเมล Phishing ออกไปลงบนฐานข้อมูล Google Sheet และช่วงที่สองคือสถานะการไม่ตอบสนอง ต่อลิงก์ Phishing หลังผู้ใช้ไม่ตอบสนองต่อลิงก์ดังกล่าวครบ 7 วัน

ตารางที่ 3-3 วิธีการเก็บค่าและเป้าหมายความสำเร็จของกรณีที่ 2

สิ่งที่เก็บ	แหล่งที่มา
เวลาที่ผู้วิจัยส่งอีเมล Phishing ออกไปลงบนฐานข้อมูล Google Sheet ด้วยตนเอง	บันทึกวันและเวลาการดำเนินการส่งอีเมลโดยผู้วิจัย
สถานะการไม่ตอบสนองต่อลิงก์ Phishing หลังผู้ใช้ไม่ตอบสนองต่อลิงก์ดังกล่าวภายใน 7 วัน	บันทึกวันและเวลาการดำเนินการโดยผู้วิจัยเมื่อครบ 7 วัน

3.5.1.1.2 วิธีการวัดผลสำหรับการโจมตีจำลองแบบ Bruteforce สามารถวัดได้จากเวลาตอบสนองของผู้ใช้ (User Response Time) ด้วยการโจมตีแบบ Bruteforce ไปยังผู้ใช้ และคำนวณการโจมตีแบบ Bruteforce แสดงดังสมการที่ 3-4

$$T_{Response} = T_{Acknowledge} - T_{Sent} \quad (3\text{-}4)$$

เมื่อ $T_{Response}$ คือ เวลาตอบสนองของผู้ใช้

$T_{Acknowledge}$ คือ เวลาที่ผู้ใช้ลงมือเปลี่ยนรหัสผ่านบนระบบรายงานการถูกโจมตี (Report System)

T_{Sent} คือ เวลาที่ผู้วิจัยส่งการแจ้งเตือนแบบ Bruteforce

จากสมการที่ 3-4 สามารถอธิบายได้ว่า ระยะเวลาตอบสนองนี้ถูกคำนวณจากความแตกต่างระหว่างเวลาที่ผู้ใช้ลงมือเปลี่ยนรหัสผ่านบนระบบรายงานการถูกโจมตี (Report System) จากบันทึกเหตุการณ์ของระบบใน Wazuh Agent บนเครื่องผู้ใช้ ลบออกจาก เวลาที่ผู้วิจัยส่งการแจ้งเตือนแบบ Bruteforce จากบันทึกเหตุการณ์ของระบบของ n8n ทั้งนี้ผู้ใช้จะต้องลงมือเปลี่ยนรหัสผ่านบนระบบรายงานภายใน 90 วินาที นับตั้งแต่ได้รับการแจ้งเตือนแบบ Bruteforce ซึ่งวัตถุประสงค์หลักของการวัดผลในขั้นตอนนี้ เพื่อยืนยันว่าผู้ใช้งานมีความตระหนักรู้ ด้านความปลอดภัย (Security Awearness) เกี่ยวกับการ Bruteforce ตามคำแนะนำได้อย่าง รวดเร็วและถูกต้อง

3.5.1.2 การคำนวณอัตราการตอบสนองต่อภัยคุกคามได้ถูกต้อง (Correct Response Rate) สามารถคำนวณได้จากการดำเนินการที่ถูกต้องต่อภัยคุกคามที่ได้รับการคำนวณค่าดังกล่าวมีความสำคัญเพื่อยืนยันว่าผู้ใช้งานมีความตระหนักรู้ด้านความปลอดภัย (Security Awearness) และสามารถดำเนินการตอบสนองต่อภัยคุกคามได้อย่างถูกต้องตามวัตถุประสงค์ของการวิจัย

3.5.1.2.1 เกณฑ์การให้คะแนนของ Phishing ผู้วิจัยมีสูตรในการคำนวณแสดงดังสมการที่ 3-5

$$R_{Correct} = (\frac{N_{Correct}}{N_{Total)}})x\ 100 \quad (3\text{-}5)$$

เมื่อ $R_{Correct}$ คือ อัตราการตอบสนองที่ถูกต้อง

$N_{Correct}$ คือ จำนวนครั้งที่ผู้ใช้งานดำเนินการตอบสนองได้ถูกต้อง

N_{Total} คือ จำนวนการโจมตีจำลองทั้งหมดที่ผู้ใช้ได้รับ

จากสมการที่ 3-5 สามารถอธิบายได้ว่า อัตราการตอบสนองที่ถูกต้องสามารถคำนวณได้จากจำนวนครั้งที่ทำถูก ซึ่งประกอบไปด้วย 2 กรณีสำหรับการโจมตีแบบอีเมล Phishing คือ ก) ผู้ใช้เพิกเฉยต่ออีเมล Phishing ข) ผู้ใช้เผลอกดลิงก์ Phishing บนอีเมล Phishing จำลองแต่สามารถเปลี่ยนรหัสผ่านได้ภายในเวลาที่กำหนด เมื่อได้จำนวนครั้งที่ทำถูกแล้ว ให้นำค่าดังกล่าวไปหารด้วยจำนวนการโจมตีจำลองทั้งหมดของผู้ใช้คนหนึ่ง จากนั้นเอาผลลัพธ์ที่หารได้ไปคูณ 100 เพื่อให้ได้อัตราการตอบสนองที่ถูกต้องในรูปแบบร้อยละ ซึ่งต้องมากกว่า 70% จึงจะถือว่าผู้ใช้มีอัตราการตอบสนอง ที่ถูกต้องอยู่ในระดับที่ผ่านเกณฑ์ ทั้งนี้วัตถุประสงค์หลักของการคำนวณในขั้นตอนนี้เพื่อยืนยันว่าผู้ใช้มีความตระหนักรู้ด้านความปลอดภัย (Security Awearness) เกี่ยวกับการตอบสนองต่อภัยคุกคามแบบ Phishing ตามคำแนะนำได้อย่างรวดเร็วและถูกต้อง

3.5.1.2.2 เกณฑ์การให้คะแนนของ Bruteforce ผู้วิจัยมีสูตรในการคำนวณแสดงดังสมการที่ 3-6

$$R_{Correct} = (\frac{N_{Correct}}{N_{Total)}})x\ 100 \quad (3\text{-}6)$$

เมื่อ $R_{Correct}$ คือ อัตราการตอบสนองที่ถูกต้อง

$N_{Correct}$ คือ จำนวนครั้งที่ผู้ใช้งานดำเนินการตอบสนองได้ถูกต้อง

N_{Total} คือ จำนวนการโจมตีจำลองทั้งหมดที่ผู้ใช้ได้รับ

จากสมการที่ 3-6 สามารถอธิบายได้ว่า อัตราการตอบสนองที่ถูกต้องสามารถคำนวณได้จากจำนวนครั้งที่ทำถูก ซึ่งได้มาจากการที่ผู้ใช้เปลี่ยนรหัสผ่านได้ทันภายในเวลา 90 วินาทีหลังจากได้รับการแจ้งเตือนภัยคุกคามแบบ Bruteforce เมื่อได้จำนวนครั้งที่ทำถูกแล้ว ให้นำค่าดังกล่าวไปหารด้วยจำนวนการโจมตีจำลองทั้งหมดของผู้ใช้คนหนึ่ง จากนั้นเอาผลลัพธ์ที่หารได้ไปคูณ 100 เพื่อให้ได้อัตราการตอบสนองที่ถูกต้องในรูปแบบร้อยละ ซึ่งต้องมากกว่า 70% จึงจะถือว่าผู้ใช้มีอัตราการตอบสนองที่ถูกต้องอยู่ในระดับที่ผ่านเกณฑ์ ทั้งนี้วัตถุประสงค์หลักของการคำนวณในขั้นตอนนี้เพื่อยืนยันว่าผู้ใช้งานมีความตระหนักรู้ด้านความปลอดภัย (Security Awearness) เกี่ยวกับการตอบสนองต่อภัยคุกคามแบบ Bruteforce ตามคำแนะนำได้อย่างรวดเร็วและถูกต้อง

3.5.1.3 ความตระหนักรู้ด้านความปลอดภัย (Security Awareness Score) ของผู้ใช้เกี่ยวกับประเภทของภัยคุกคาม ความหมายของการแจ้งเตือนและขั้นตอนการตอบสนองที่ถูกต้องต่อภัยคุกคามสามารถคำนวณได้จากการใช้คะแนนจากแบบทดสอบก่อนการวิจัย (Pre-test) ที่ดำเนินการในขั้นตอน P (Plan) มาเปรียบเทียบกับ แบบทดสอบหลังการวิจัย (Post-test) ที่ดำเนินการในขั้นตอน C (Check) ของวัฏจักร PDCA เพื่อยืนยันการเพิ่มขึ้นของความตระหนักรู้ด้านความปลอดภัย (Security Awareness) เกณฑ์ 70% ถูกกำหนดขึ้นเป็นเป้าหมายความสำเร็จเพื่อใช้ยืนยันว่าผู้ใช้มีความรู้ความเข้าใจเกี่ยวกับประเภทของภัยคุกคาม ความหมายของการแจ้งเตือนและขั้นตอนการตอบสนองที่ถูกต้องต่อภัยคุกคามมากขึ้นตามวัตถุประสงค์ของการวิจัย

3.5.2 เกณฑ์วัดผลด้านระบบ (System Metrics) ใช้วัดประสิทธิภาพทางเทคนิคของระบบตรวจจับภัยคุกคาม Wazuh IDS และระบบอัตโนมัติ (n8n/AI) เพื่อยืนยันความสามารถในการทำงานที่เชื่อถือได้

3.5.2.1 ความแม่นยำในการตรวจจับ (Detection Accuracy) เป็นค่าสำหรับการวัดผลประสิทธิภาพทางเทคนิคของระบบตรวจจับภัยคุกคาม Wazuh IDS และระบบอัตโนมัติ (n8n/AI) มีไว้เพื่อยืนยันความสามารถในการทำงานที่เชื่อถือได้ของระบบ ผู้วิจัยได้ใช้ค่าทางสถิติเพื่อวัดความแม่นยำในการตรวจจับ (Detection Accuracy) ซึ่งประกอบด้วยความแม่นยำ (Precision) คือสัดส่วนของการแจ้งเตือนที่ระบบตรวจจับ (Wazuh) สร้างขึ้นซึ่งสอดคล้องกับเหตุการณ์ภัยคุกคามจำลองที่เกิดขึ้นจริง โดยมีวัตถุประสงค์เพื่อลดอัตราการแจ้งเตือนที่ผิดพลาด (False Positives) และความรำลึก (Recall) คือสัดส่วนของเหตุการณ์ภัยคุกคามจำลองที่เกิดขึ้นจริงทั้งหมดที่ระบบสามารถตรวจจับได้เพื่อลดอัตราการตรวจไม่พบ (False Negatives) นอกจากนี้ยังใช้ค่าเฉลี่ยแบบ Harmonic Mean ของ Precision และ Recall (F1-score) เพื่อให้ได้ค่าความแม่นยำที่ครอบคลุม โดยการเลือกใช้ค่าทางสถิติเหล่านี้มีความสำคัญเพื่อยืนยันความแม่นยำและความสามารถในการตรวจจับภัยคุกคามจำลองได้ครบถ้วนของระบบที่พัฒนาขึ้นตามวัตถุประสงค์ของงานวิจัย

3.5.2.2 เวลาในการตรวจจับ (Detection Time) เป็นค่าสำหรับการวัดผลด้านระบบด้วยการวัดความเร็วของระบบบูรณาการทั้งหมด โดยการวัดจะเริ่มนับจากเวลาที่ Wazuh Agent บนเครื่องผู้ใช้เริ่มเก็บบันทึกเหตุการณ์ของระบบที่สอดคล้องกับการโจมตีจำลอง (เช่น การคลิกลิงก์ Phishing หรือการโจมตี Bruteforce) และจะสิ้นสุดลงเมื่อระบบ Wazuh Server สร้างการแจ้งเตือน (Alert) และส่งข้อมูลไปยังระบบอัตโนมัติ (n8n) สำเร็จ การวัดนี้มีวัตถุประสงค์เพื่อประเมินความสามารถในการทำงานที่เชื่อถือได้ของระบบที่พัฒนาขึ้นในการสร้างการแจ้งเตือนที่รวดเร็วเพื่อส่งต่อข้อมูลไปยังส่วนประมวลผลอัตโนมัติได้ทันท่วงที

3.5.2.3 การใช้ทรัพยากรเครื่อง (System Performance) เป็นค่าสำหรับการวัดผลด้านระบบผู้วิจัยเลือกใช้วิธีการวัดเปอร์เซ็นต์การใช้ทรัพยากรเครื่อง (CPU และ Memory/RAM) ของเครื่อง Wazuh Server และ Wazuh Agent ในช่วงที่มีการโจมตีจำลอง โดยมีวัตถุประสงค์เพื่อประเมินว่าระบบที่พัฒนาขึ้นสร้างภาระ (Overhead) มากเกินไปจนส่งผลกระทบต่อการใช้งานปกติของเครื่องคอมพิวเตอร์และเครื่อง Server หรือไม่ ซึ่งการวัดผลนี้มีความสำคัญในการยืนยันความสามารถในการทำงานที่เชื่อถือได้ของระบบตรวจจับภัยคุกคาม Wazuh IDS และระบบอัตโนมัติ (n8n/AI) ตามวัตถุประสงค์ของงานวิจัย

3.5.3 รายละเอียดฐานข้อมูลสำหรับวัดผลเพื่อใช้จัดเก็บข้อมูลดิบในการคำนวณค่าตัวชี้วัดด้านผู้ใช้งานและด้านระบบในขั้นตอน C: Check ได้อย่างถูกต้อง งานวิจัยนี้ได้กำหนดโครงสร้างของฐานข้อมูลที่จัดทำด้วย Google Sheet สำหรับการโจมตีทั้งประเภท Phishing และ Bruteforce ดังนี้

3.5.3.1 ฐานข้อมูล Google Sheet สำหรับการโจมตีประเภท Phishing เพื่อให้สามารถเก็บข้อมูลได้ครบถ้วน ผู้วิจัยได้เก็บข้อมูลในหลากหลายรายการแสดงดังตารางที่ 3-4

ตารางที่ 3-4 รายละเอียดฐานข้อมูล Google Sheet สำหรับการโจมตีประเภท Phishing

ชื่อ Field	**ความหมาย**
Event_ID	รหัสเหตุการณ์
Computer_Name	ชื่อคอมพิวเตอร์
Phishing_Email_Sent	วันที่และเวลาที่ผู้วิจัยส่งอีเมล Phishing ไปยังผู้ใช้
Link_Clicked	วันที่และเวลาที่ผู้ใช้คลิกลิงก์ในอีเมล Phishing จำลอง (ระบุ "Did Not Click" หากไม่ได้คลิก)
AI_Alert_Sent_Telegram	วันที่และเวลาที่ระบบ AI ส่งการแจ้งเตือนไปยังผู้ใช้ผ่าน Telegram ในกรณีที่ผู้ใช้คลิกลิงก์ Phishing บนอีเมล Phishing จำลอง (ระบุ "N/A" หากไม่ได้คลิกลิงก์)
Acknowledge_at_report_system	วันที่และเวลาที่ผู้ใช้เปลี่ยนรหัสผ่านในระบบรายงานการโจมตี (Report System) (ระบุ "No Action Needed" หากไม่คลิกลิงก์ หรือ "No Response" หากคลิกลิงก์ Phishing แต่ไม่เปลี่ยนรหัสผ่าน)

ตารางที่ 3-4 (ต่อ)

User_Response_Time_Sec	ระยะเวลาในหน่วยวินาทีที่ผู้ใช้ใช้ในการตอบกลับ (คำนวณจาก Acknowledge_at_report_system - AI_Alert_Sent_Telegram)
Overall_Status	ผลลัพธ์ของการตอบสนองสามารถแบ่งสถานะออกได้เป็น 4 รูปแบบ โดยCorrect คือการดำเนินการถูกต้อง (ไม่คลิกลิงก์) Correct (Response) / Incorrect (Action) คือ ผู้ใช้เผลอคลิกลิงก์แต่เปลี่ยนรหัสผ่านทันเวลา Incorrect (Ignored) คือ คลิกลิงก์แต่ไม่เปลี่ยนรหัสผ่าน และ Incorrect (Delay) คือคลิกลิงก์แต่เปลี่ยนรหัสผ่านไม่ทันเวลาที่กำหนด

จากตารางที่ 3-4 แสดงถึงรายละเอียดโครงสร้างของฐานข้อมูล Phishing ซึ่งถูกจัดทำขึ้นด้วย Google Sheet เพื่อใช้จัดเก็บข้อมูลดิบทั้งหมดที่เกี่ยวข้องกับการโจมตีจำลองแบบ Phishing สำหรับนำไปคำนวณค่าตัวชี้วัดด้านผู้ใช้งานและด้านระบบ โดยระบุรายละเอียดของแต่ละ Field ตั้งแต่เวลาที่ผู้วิจัยส่งอีเมลไปจนถึงผลลัพธ์ของการตอบสนองโดยรวม (Overall Status)

3.5.3.2 ฐานข้อมูล Google Sheet สำหรับการโจมตีประเภท Bruteforce เพื่อให้สามารถเก็บข้อมูลได้ครบถ้วน ผู้วิจัยได้เก็บข้อมูลในหลากหลายรายการแสดงดังตารางที่ 3-5

ตารางที่ 3-5 รายละเอียดฐานข้อมูล Google Sheet สำหรับการโจมตีประเภท Bruteforce

ชื่อ Field	ความหมาย
Event_ID	รหัสเหตุการณ์
Computer_Name	ชื่อคอมพิวเตอร์
Sent_Bruteforce	วันที่และเวลาที่ผู้วิจัยส่งการโจมตีจำลองแบบ Bruteforce ไปยังผู้ใช้ผ่าน Telegram
Password_Changed_at_report_system	เวลาที่ผู้ใช้เปลี่ยนรหัสผ่านในระบบรายงานการถูกโจมตี (Report System) (หรือ 'No Response' ถ้าไม่มีการตอบสนอง)

ตารางที่ 3-5 (ต่อ)

User_Response_Time_Sec	ระยะเวลาในหน่วยวินาทีที่ผู้ใช้ใช้ในการตอบกลับ (คำนวณจาก Password_Changed_at_report_system - Sent_Bruteforce) หรือ 'N/A' ถ้าไม่มีการตอบสนอง
Result	ผลลัพธ์ของการตอบสนองสามารถแบ่งสถานะออกได้เป็น 3 รูปแบบ โดย Correct คือการดำเนินการถูกต้อง (เปลี่ยนรหัสผ่านทันเวลา) Incorrect (Delay) คือการดำเนินการไม่ถูกต้อง (เปลี่ยนรหัสผ่านไม่ทันเวลาที่กำหนด) และ Incorrect (Ignored) คือการดำเนินการไม่ถูกต้อง (ไม่เปลี่ยนรหัสผ่าน)

จากตารางที่ 3-5 แสดงถึงรายละเอียดโครงสร้างของฐานข้อมูล Bruteforce ซึ่งถูกจัดทำขึ้นด้วย Google Sheet เพื่อใช้จัดเก็บข้อมูลดิบทั้งหมดที่เกี่ยวข้องกับการโจมตีจำลองแบบ Bruteforce สำหรับนำไปคำนวณค่าตัวชี้วัดด้านผู้ใช้งานและด้านระบบ โดยระบุรายละเอียดของแต่ละ Field ตั้งแต่เวลาที่ผู้วิจัยส่งการโจมตีจำลอง (Sent Bruteforce) ไปจนถึงผลลัพธ์ของการตอบสนอง (Result) ซึ่งรวมถึงระยะเวลาการตอบสนองของผู้ใช้ (User Response Time) เพื่อวัดว่าผู้ใช้เปลี่ยนรหัสผ่านได้ทันภายในระยะเวลาที่กำหนดหรือไม่

3.6 ขั้นตอนการดำเนินงานวิจัยตามวัฏจักร PDCA

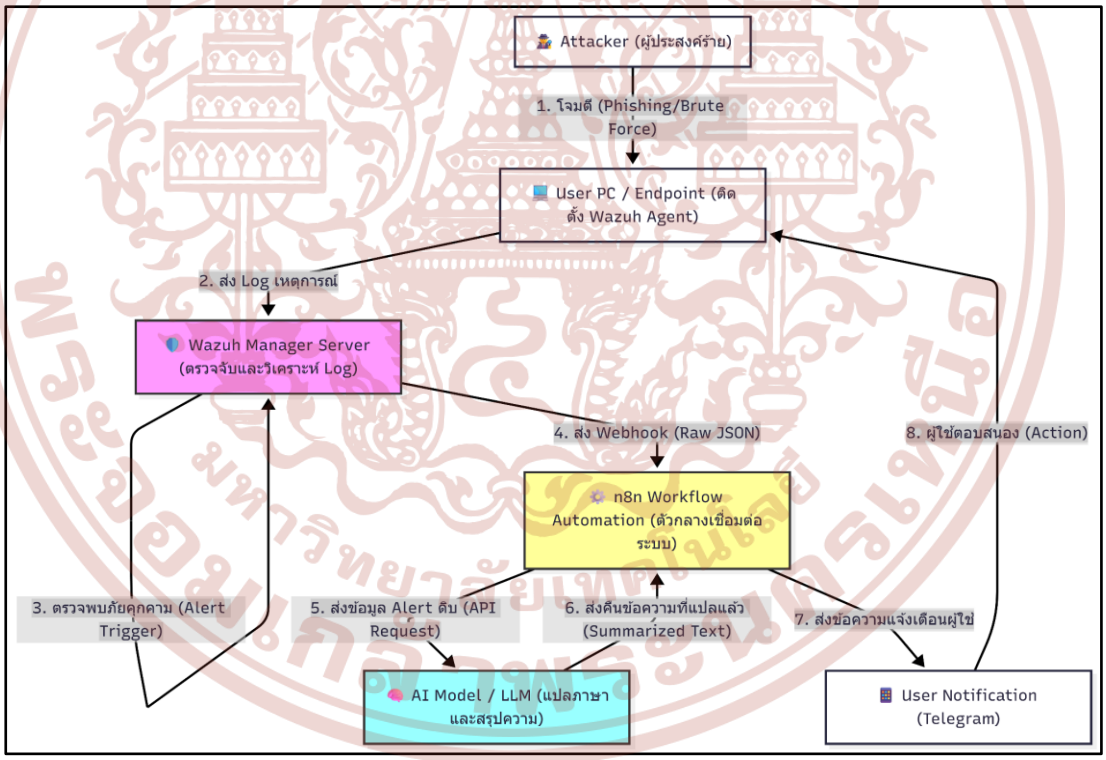
การดำเนินงานวิจัยนี้เป็นไปตามวัฏจักร PDCA ซึ่งเป็นกรอบการปรับปรุงอย่างต่อเนื่องโดยมีรายละเอียดขั้นตอนดังนี้

3.6.1 P: Plan (การวางแผน)

3.6.1.1 ทบทวนวรรณกรรมและการออกแบบระบบโดยการศึกษาแนวคิดและวิธีการใช้งานเครื่องมือ Open-Source เกี่ยวกับเรื่องความปลอดภัยและระบบอัตโนมัติอย่าง Wazuh IDS, Workflow Automation จาก n8n และปัญญาประดิษฐ์เพื่อออกแบบสถาปัตยกรรมระบบต้นแบบให้สามารถเชื่อมโยง Wazuh IDS เข้ากับ Workflow Automation จาก n8n และปัญญาประดิษฐ์ได้

3.6.1.2 การออกแบบผังการทำงานระบบแจ้งเตือน (System Workflow) ประกอบด้วยสามส่วนหลักตามลำดับ โดยเริ่มต้นที่ส่วนตรวจจับ (Detection Layer) ซึ่ง Wazuh Agent จะทำหน้าที่เก็บบันทึกเหตุการณ์ของระบบจากเครื่องลูกข่ายของผู้ใช้เพื่อส่งบันทึกเหตุการณ์ไปยัง

Wazuh Server จากนั้น Wazuh Server จะสร้างการแจ้งเตือนตามกฎที่กำหนดไว้ การแจ้งเตือนดังกล่าวจะถูกส่งต่อไปยังส่วนประมวลผลอัตโนมัติ (Workflow Automation Layer) บน Workflow n8n โดย n8n มีหน้าที่ในการรับการแจ้งเตือนดิบ (Raw JSON) จาก Wazuh Server ที่ถูกส่งมาจากส่วนตรวจจับ (Detection Layer) ก่อนจะส่งต่อให้ปัญญาประดิษฐ์ภายใน Workflow n8n เพื่อดำเนินการแปลผลให้เป็นข้อความที่กระชับและเข้าใจง่าย จากนั้น Workflow n8n จะส่งข้อความแจ้งเตือนที่แปลผลแล้วจากส่วนประมวลผลอัตโนมัติ ก่อนหน้าไปยังผู้ใช้ผ่าน Telegram เพื่อให้ผู้ใช้ดำเนินการแก้ไขได้อย่างถูกต้องและทันท่วงที และสุดท้ายคือส่วนการตอบสนอง (Response Layer) ที่ผู้ใช้จะได้รับข้อความที่ถูกแปลผลจาก AI และดำเนินการตอบสนองภัยคุกคาม ดังนี้ผลการตอบสนองทั้งหมดจะถูกบันทึกโดย Wazuh Agent และนำมาเป็นตัวชี้วัดสำคัญของงานวิจัยทั้งด้านผู้ใช้งานและด้านระบบต่อไปแสดงดังภาพที่ 3-1



ภาพที่ 3-1 ผังการทำงานระบบแจ้งเตือน (System Workflow)

จากผังข้างต้น กระบวนการทำงานจะแบ่งออกเป็น 3 ส่วนหลักได้แก่ ส่วนตรวจจับ (Detection Layer) ส่วนประมวลผลอัตโนมัติ (Automation & Intelligence Layer) และส่วนการตอบสนอง (Response Layer) มีรายละเอียดดังนี้

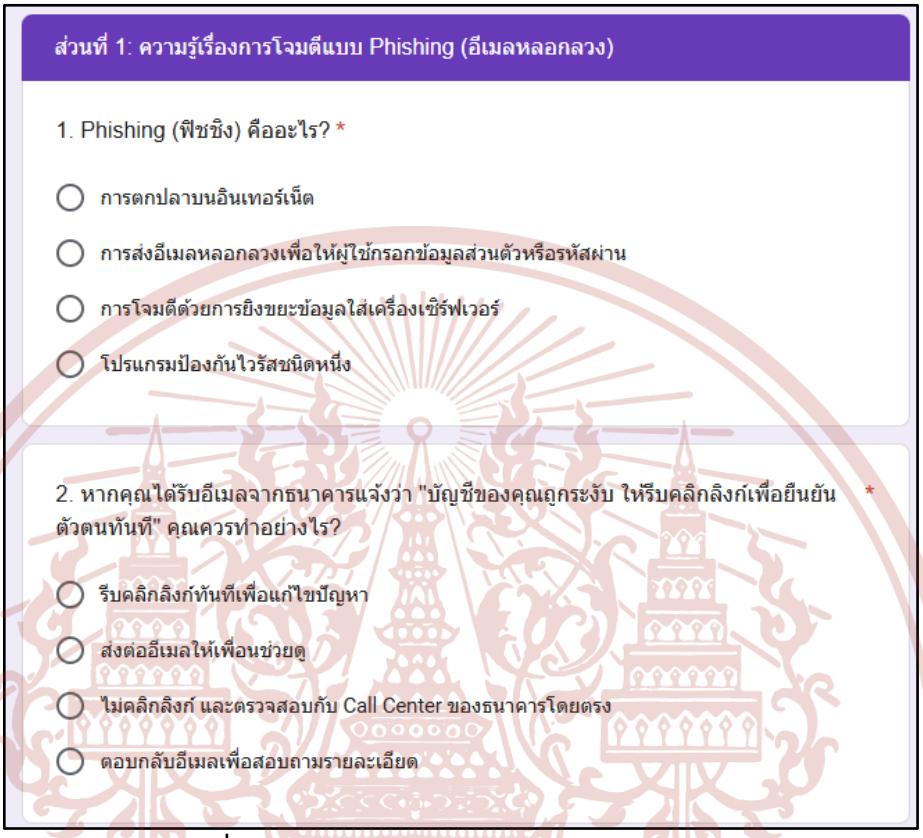
3.1.6.2.1 ส่วนตรวจจับ (Detection Layer) เริ่มต้นด้วยการที่ผู้วิจัยจะจำลองเป็นผู้ประสงค์ร้ายส่งอีเมล Phishing หรือส่งการแจ้งเตือน Bruteforce ไปยังผู้ใช้ เมื่อผู้ใช้คลิก

ลิงก์บนอีเมล Phishing จำลองหรือคลิกลิงก์สำหรับเปลี่ยนรหัสผ่านบนข้อความแจ้งเตือนภัยคุกคามแบบ Bruteforce จะทำให้ Wazuh Agent ที่ติดตั้งอยู่บนเครื่องผู้ใช้จะทำหน้าที่เก็บบันทึกเหตุการณ์ของระบบนั้นไว้และส่งบันทึกเหตุการณ์นั้นไปยัง Wazuh Server เมื่อข้อมูลมาถึง Wazuh Server แล้วระบบจะเปรียบเทียบบันทึกเหตุการณ์ของระบบที่ได้รับกับกฎที่กำหนดไว้ (เว็บไซต์รายงานการถูกโจมตีหรือลิงก์ Phishing) หากตรงกัน Wazuh Server จะสร้างการแจ้งเตือนดิบ (Raw JSON) ขึ้นมาเพื่อเตรียมส่งไปยัง n8n ในขั้นตอนประมวลผลอัตโนมัติต่อไป

3.1.6.2.2 ส่วนประมวลผลอัตโนมัติ (Automation & Intelligence Layer) เริ่มต้นด้วยการส่งเนื้อหา โดย Wazuh Server จะส่งการแจ้งเตือนดิบ (Raw JSON) ผ่าน Webhook ไปยัง n8n ซึ่งทำหน้าที่เป็น Workflow ในการรับข้อมูลและส่งต่อไปยังปัญญาประดิษฐ์ โดยมีวัตถุประสงค์เพื่อให้ AI ทำหน้าที่เป็น "ล่าม" แปลศัพท์เทคนิคที่ซับซ้อนให้เป็นภาษามนุษย์ที่เข้าใจง่ายและสรุปคำแนะนำในการแก้ไขปัญหาเพื่อลดช่องว่างระหว่างการมีผู้เชี่ยวชาญ ด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์ในองค์กรกับผู้ใช้งานทั่วไป และสุดท้ายข้อความที่ถูกแปลผลจาก AI นั้นจะถูกส่งกลับมาที่ n8n Workflow จากนั้น n8n Workflow จะส่งข้อความแจ้งเตือนที่ถูกแปลผลจาก AI ไปยังผู้ใช้ผ่าน Telegram ซึ่งมีวัตถุประสงค์เพื่อให้ผู้ใช้สามารถตอบสนองต่อภัยคุกคามได้อย่างถูกต้อง

3.1.6.2.3 ส่วนการตอบสนอง (Response Layer) เริ่มต้นด้วยการที่ผู้ใช้ได้รับข้อความที่ถูกแปลผลจาก AI ในขั้นตอนก่อนหน้าและดำเนินการตอบสนองภัยคุกคามด้วยการเปลี่ยนรหัสผ่าน โดยผลการตอบสนองทั้งหมดจะถูกบันทึกโดย Wazuh Agent ที่อยู่บนเครื่องลูกข่ายของผู้ใช้และนำมาเป็นตัวชี้วัดสำคัญของงานวิจัยทั้งด้านผู้ใช้งานและด้านระบบต่อไป

3.6.1.3 การอบรมและจัดเตรียมเครื่องมือวัดผล ผู้วิจัยได้จัดทำวิดีโอเกี่ยวกับความตระหนักรู้ด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์เพื่อให้ผู้ใช้มีความรู้ความเข้าใจพื้นฐานเกี่ยวกับเรื่องดังกล่าวและยังได้จัดทำคู่มือการตอบสนองต่อภัยคุกคามที่ถูกต้อง เพื่อให้ผู้ใช้สามารถตอบสนองต่อภัยคุกคามได้อย่างถูกต้องภายในเวลาที่กำหนด ต่อมาผู้วิจัยได้ดำเนินการออกแบบชุดแบบทดสอบก่อนการทดลอง (Pre-test) และแบบทดสอบหลังการทดลอง (Post-test) เพื่อวัดความรู้ความเข้าใจด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์ ลำดับถัดไปผู้วิจัยจะดำเนินการทดสอบก่อนการทดลอง (Pre-test) ให้กับผู้ใช้และบันทึกคะแนนเริ่มต้นไว้เป็นค่าเปรียบเทียบกับการทดสอบหลังการทดลอง (Post-test) ในขั้นตอน Check ซึ่งเป็นตัวบ่งชี้การเพิ่มขึ้นของความตระหนักรู้ด้านความปลอดภัย (Security Awareness Score) ตามวัตถุประสงค์ของงานวิจัย พร้อมกันนี้ยังมีการจัดทำเกณฑ์วัดผลด้านผู้ใช้งานและด้านระบบอย่างชัดเจนเพื่อกำหนดชุดตัวชี้วัดที่เชื่อถือได้สำหรับการประเมินทั้งประสิทธิภาพของการตอบสนองของผู้ใช้และประสิทธิภาพทางเทคนิคของระบบ ซึ่งแบบทดสอบก่อน/หลังการทดลองแสดงดังภาพที่ 3-2



ภาพที่ 3-2 ตัวอย่างแบบทดสอบก่อน/หลังการทดลอง

3.6.1.4 การวางแผนสถาปัตยกรรมและการตั้งค่าระบบประกอบด้วยองค์ประกอบหลักที่สำคัญต่อการทำงานร่วมกันของระบบบูรณาการทั้งสามส่วนดังนี้

3.6.1.4.1 การกำหนดแผนการติดตั้งและเก็บข้อมูลของ Wazuh Agents บนเครื่องลูกข่ายของผู้ใช้งานเพื่อให้ Agent ทำหน้าที่เก็บบันทึกเหตุการณ์ของระบบผู้ใช้ เช่น บันทึกเหตุการณ์การเข้าถึงเว็บไซต์ระบบรายงานการถูกโจมตีหรือการคลิกลิงก์ Phishing เป็นต้น เมื่อผู้ใช้ดำเนินการอย่างใดอย่างหนึ่งตามที่กล่าวไป Wazuh Agent จะส่งบันทึกเหตุการณ์ของระบบไปยัง Wazuh Server เพื่อให้ Server เก็บข้อมูลนั้นไว้ ดังนั้นข้อมูลบันทึกเหตุการณ์ของระบบนี้จำเป็นต่อการบันทึกพฤติกรรมและการคำนวณตัวชี้วัดต่างๆ ตามวัตถุประสงค์ของงานวิจัย

3.6.1.4.2 การออกแบบและกำหนดค่าเบื้องต้นฝั่ง Server (Wazuh Server, n8n, AI) ในขั้นตอน P: Plan (การวางแผน) เป็นสิ่งสำคัญอย่างยิ่งในการสร้างกระบวนการบูรณาการร่วมกันของ Wazuh, n8n และ AI โดยมีเหตุผลในการดำเนินการดังนี้

ก) การตั้งค่า Wazuh Server สำหรับการส่งข้อมูลไปยัง n8n ต้องเริ่มจากการกำหนดรายละเอียดในไฟล์ ossec.conf บน Wazuh Server มีวัตถุประสงค์เพื่อให้ระบบสามารถส่งการแจ้งเตือนดิบ (Raw JSON) ผ่าน Webhook ไปยังระบบอัตโนมัติ n8n ได้โดยอัตโนมัติ

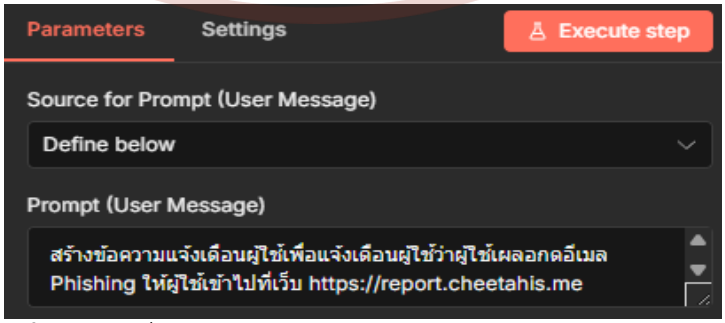
ข) การตั้งค่า Wazuh Server สำหรับการตั้งค่ากฎให้ตรวจจับการเข้าเว็บไซต์ Phishing หรือระบบรายงานการถูกโจมตี (Report System) ซึ่งต้องกำหนดรายละเอียดในไฟล์ local_rules.xml ของ Wazuh Server เพื่อให้ Server สร้างการแจ้งเตือนและส่งต่อไปยัง Workflow n8n ที่ออกแบบไว้ต่อไป

ค) กำหนดให้ n8n ทำหน้าที่เป็น Workflow เพื่อรับข้อมูลดิบจาก Wazuh Server และส่งต่อให้ปัญญาประดิษฐ์ จากนั้นจึงนำข้อมูลที่ได้รับกลับมาจากปัญญาประดิษฐ์ส่งต่อไปยังผู้ใช้ผ่าน Telegram ต่อไป

ง) ท้ายที่สุดผู้วิจัยได้จัดทำฐานข้อมูล Phishing และฐานข้อมูล Bruteforce ด้วย Google Sheet เพื่อเก็บข้อมูลการจำลองการโจมตีของ งานวิจัยนี้จาก Workflow n8n

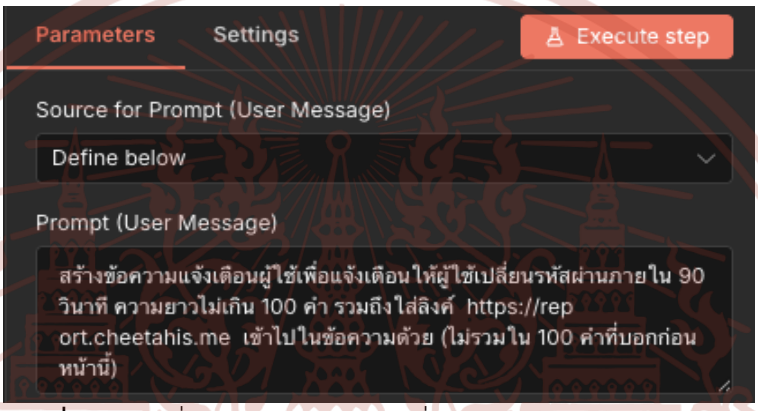
3.6.1.4.3 กำหนดรายละเอียดของคำสั่งเฉพาะสำหรับปัญญาประดิษฐ์ (AI Prompt) ซึ่งทำงานอยู่ในระบบ Workflow n8n เพื่อทำหน้าที่เป็น "ล่าม" ในการแปลการแจ้งเตือนภัยคุกคามทางเทคนิคที่ซับซ้อนจาก Wazuh IDS ให้เป็นข้อความแจ้งเตือนที่ชัดเจนกระชับและให้คำแนะนำที่ต้องดำเนินการทันทีแก่ผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญผ่าน Telegram แบ่งออกเป็น 2 ประเภทดังนี้

ก) คำสั่ง (Prompt) ของเหตุการณ์เมื่อผู้ใช้เผลอกดลิงก์ Phishing บนอีเมล Phishing จำลองคือ "สร้างข้อความแจ้งเตือนผู้ใช้เพื่อเตือนให้ผู้ใช้ว่าผู้ใช้เผลอกดอีเมล Phishing ให้ผู้ใช้เข้าไปที่เว็บระบบรายงานการถูกโจมตีเพื่อเปลี่ยนรหัสผ่าน ภายใน 90 วินาที" คำสั่งดังกล่าวมีไว้เพื่อให้ AI สร้างข้อความแจ้งเตือนสำหรับแจ้งเตือนผู้ใช้ให้เข้าไปที่ระบบรายงานการถูกโจมตีและกดเปลี่ยนรหัสผ่านภายใน 90 วินาที แสดงดังภาพที่ 3-3



ภาพที่ 3-3 คำสั่ง (Prompt) สำหรับแจ้งเตือนผู้ใช้หลังกดลิงก์ Phishing

ข) คำสั่ง (Prompt) ของเหตุการณ์เมื่อผู้วิจัยกดปุ่ม “เริ่มต้นส่งข้อความแบบ Bruteforce” บน Workflow n8n คือ “สร้างข้อความแจ้งเตือนผู้ใช้เพื่อแจ้งเตือนให้ผู้ใช้เปลี่ยนรหัสผ่านภายใน 90 วินาที ความยาวไม่เกิน 100 คำ รวมถึงใส่ลิงก์ระบบรายงานการถูกโจมตีเข้าไปในข้อความด้วย (ไม่รวมใน 100 คำที่บอกก่อนหน้านี้)” คำสั่งดังกล่าวมีไว้เพื่อแจ้งเตือนให้ผู้ใช้เปลี่ยนรหัสผ่านหลังจากถูกโจมตีแบบ Bruteforce แสดงดังภาพที่ 3-4



ภาพที่ 3-4 คำสั่ง (Prompt) สำหรับเริ่มโจมตีผู้ใช้ด้วยวิธี Bruteforce

3.6.1.5 การจัดเตรียมเครื่องมือการโจมตีและการตอบสนองมีทั้งหมดสองประเภทดังนี้

3.6.1.5.1 การโจมตีประเภท Phishing

ก) ออกแบบอีเมล Phishing จำนวน 15 รูปแบบที่สมจริงและมุ่งเป้าโดยตรง เช่น การแจ้งเตือนบัญชีหมดอายุ มีวัตถุประสงค์เพื่อจำลองสถานการณ์ภัยคุกคามจริงและหลอกล่อให้ผู้ใช้คลิกลิงก์ที่เกี่ยวข้องกับการทำงานประจำวันเพื่อวัดความสามารถของผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญในการระบุภัยคุกคามและตอบสนองได้อย่างถูกต้องแสดงดังภาพที่ 3-5



ต้องดำเนินการด่วน: ยืนยันบัญชี AWS ของคุณเพื่อหลีกเลี่ยงการระงับบัญชี

เรียนคุณ ลูกค้า AWS,

ระบบของเราระบุว่ามีปัญหาเร่งด่วนเกี่ยวกับบัญชี AWS ของคุณที่ต้องการการยืนยันทันที หากไม่ยืนยันบัญชีของคุณ อาจส่งผลให้บริการ AWS ของคุณถูกระงับ

โปรดยืนยันบัญชีของคุณโดยคลิกลิงก์ด้านล่าง:

คลิกที่นี่เพื่อยืนยันบัญชี AWS ของคุณ

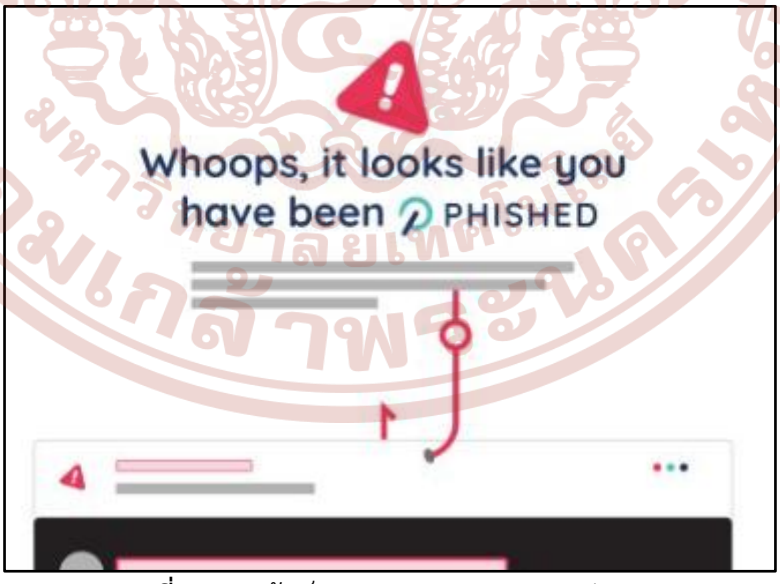
เราขอแนะนำอย่างยิ่งให้ทำกระบวนการยืนยันนี้ให้เสร็จสิ้นภายใน 24 ชั่วโมงหลังจากได้รับอีเมลนี้ เพื่อให้มั่นใจว่าคุณสามารถเข้าถึงทรัพยากร AWS ของคุณได้อย่างต่อเนื่อง

ขอบคุณสำหรับความสนใจในเรื่องนี้อย่างรวดเร็ว

ด้วยความนับถือ,
ทีมสนับสนุน AWS

ภาพที่ 3-5 ตัวอย่างอีเมล Phishing จำลอง

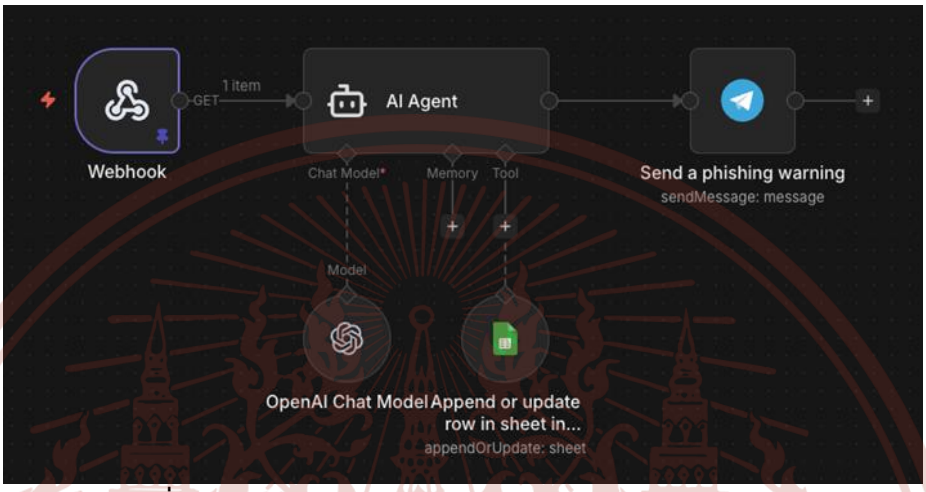
ข) สร้างหน้าเว็บจำลองฟิชชิ่งสำหรับอบรม (Phishing Landing Page) และลิงก์ของหน้าเว็บนั้นเพื่อใช้แนบไปกับอีเมล Phishing จำลองที่ส่งหาผู้ใช้ในข้อก่อนหน้า มีวัตถุประสงค์เพื่อจำลองสถานการณ์ภัยคุกคามไซเบอร์จริงเพื่อให้ผู้ได้เผชิญกับสถานการณ์จริง และวัดผลการตอบสนองของพวกเขาแสดงดังภาพที่ 3-6



ภาพที่ 3-6 หน้าเว็บจำลอง Phishing สำหรับอบรม

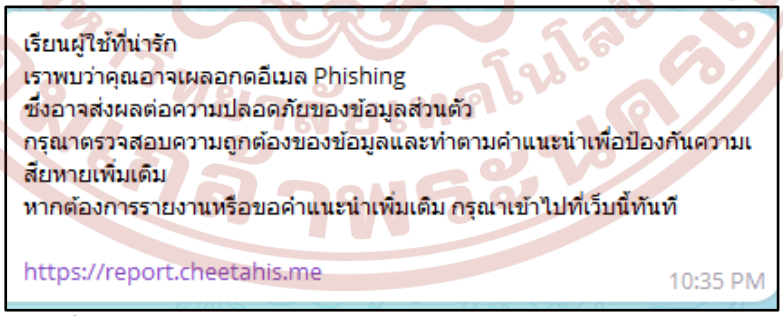
ค) สร้าง Workflow ใน n8n สำหรับการรับการแจ้งเตือนดิบ (Raw JSON) จาก Wazuh Server แล้วส่งต่อให้ AI เป็น "ล่าม" แปลศัพท์เทคนิคให้เป็นข้อความแจ้งเตือน

ที่เข้าใจง่าย ชัดเจนและกระชับ พร้อมคำแนะนำการเปลี่ยนรหัสผ่านที่ต้องทำทันที ก่อนส่งถึงผู้ใช้แสดงดังภาพที่ 3-7



ภาพที่ 3-7 Workflow สำหรับรับจากแจ้งเตือนมาทำ Phishing

ง) สร้างข้อความแจ้งเตือนสำหรับส่งให้ผู้ใช้ที่เผลอคลิกลิงก์ Phishing ในอีเมล Phishing จำลอง โดยใช้คำสั่ง (Prompt) ที่อยู่ภายใต้หัวข้อ 3.6.1.4.3 กำหนดรายละเอียดของคำสั่งเฉพาะสำหรับปัญญาประดิษฐ์ (AI Prompt) เพื่อใช้สำหรับการส่งข้อความแจ้งเตือนดังกล่าวไปยังผู้ใช้เพื่อให้ผู้ใช้ดำเนินการเปลี่ยนรหัสผ่านและเก็บบันทึกรายละเอียดสำหรับวัดผลตามวัตถุประสงค์ของการวิจัย แสดงดังภาพที่ 3-8



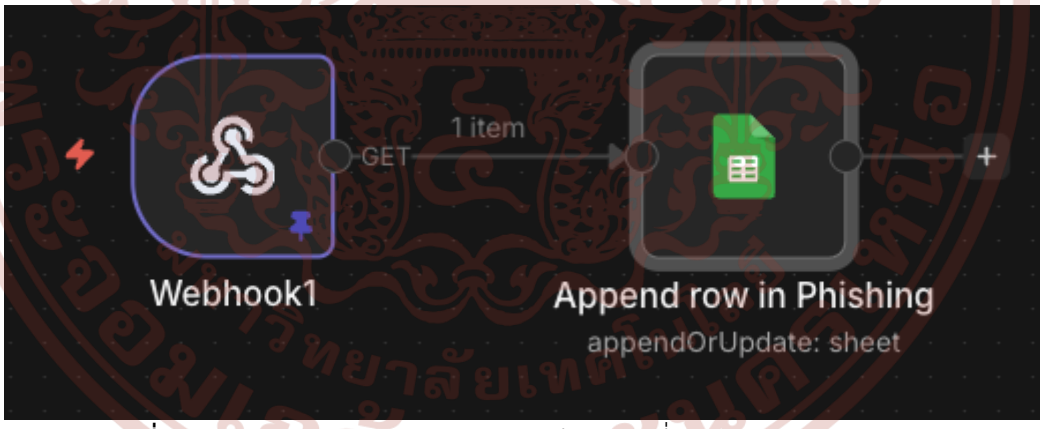
ภาพที่ 3-8 ตัวอย่างผลลัพธ์ข้อความแจ้งเตือนผู้ใช้ในการทำ Phishing

จ) สร้างระบบสำหรับรายงานการถูกโจมตี (Report System) เพื่อให้ผู้ใช้ที่คลิกลิงก์ในข้อความแจ้งเตือนในข้อก่อนหน้าสามารถเข้ามาดำเนินการเปลี่ยนรหัสผ่านตามคำแนะนำที่ผู้วิจัยได้อบรมไว้แสดงดังภาพที่ 3-9



ภาพที่ 3-9 ระบบรายงานการถูกโจมตี (Report System)

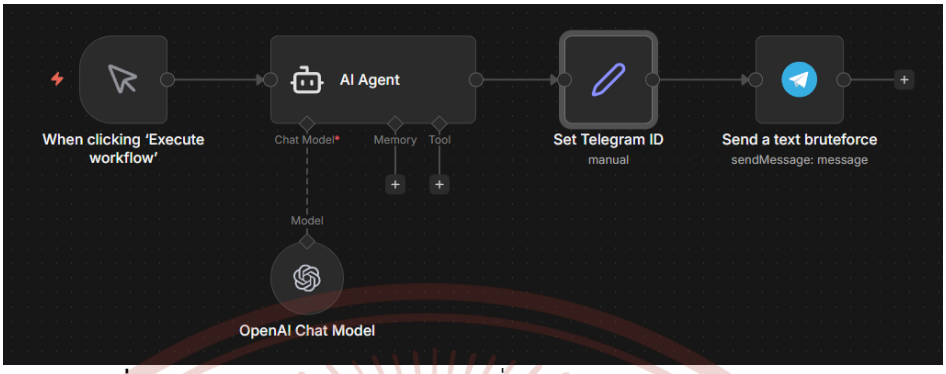
ฉ) สร้าง Workflow ใน n8n เพื่อรับการแจ้งเตือนดิบจาก Wazuh Server ผ่าน Webhook หลังจากที่ผู้ใช้ได้เข้ามาเปลี่ยนรหัสผ่านในระบบรายงานในข้อก่อนหน้า โดย Workflow ดังกล่าวจะบันทึกเวลาตอบสนองของผู้ใช้ลงในฐานข้อมูล Google Sheet ที่เตรียมไว้ และนำไปใช้คำนวณเวลาตอบสนองของผู้ใช้และยืนยันความตระหนักรู้ด้านความปลอดภัยต่อไป แสดงดังภาพที่ 3-10



ภาพที่ 3-10 Workflow n8n สำหรับบันทึกการเปลี่ยนรหัสผ่านของ Phishing

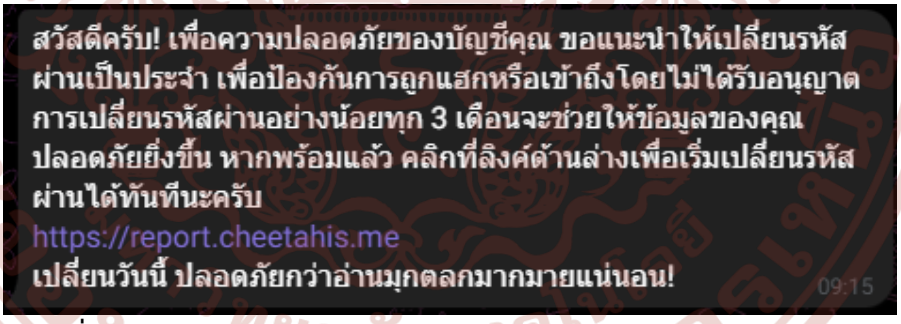
3.6.1.5.2 การโจมตีประเภท Phishing

ก) สร้าง Workflow ใน n8n สำหรับใช้จำลองการแจ้งเตือนภัย Bruteforce โดยเมื่อผู้วิจัยกดปุ่มเริ่มการทำงาน Workflow จะให้ AI/LLM ส่งการแจ้งเตือนที่เข้าใจง่ายและกระชับก่อนส่งผ่าน Telegram พร้อมลิงก์ระบบรายงานเพื่อกระตุ้นให้ผู้ใช้เปลี่ยนรหัสผ่านทันที แสดงดังภาพที่ 3-11



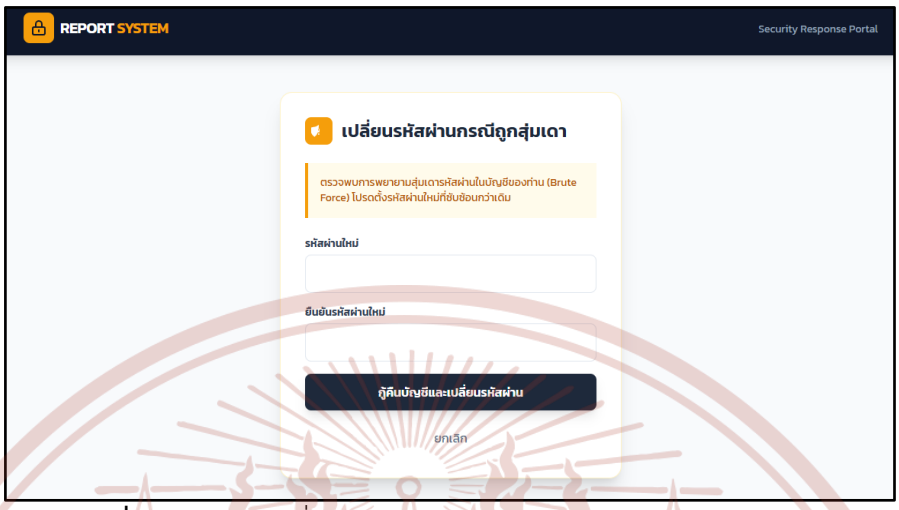
ภาพที่ 3-11 Workflow n8n สำหรับเริ่มการโจมตีจำลองของ Bruteforce

ข) สร้างข้อความแจ้งเตือนสำหรับส่งไปแจ้งเตือนให้ผู้ใช้เปลี่ยนรหัสผ่านเนื่องจากโดนโจมตีแบบ Bruteforce โดยใช้คำสั่ง (Prompt) ที่กำหนดไว้ใน หัวข้อ **Bruteforce** ที่อยู่ภายใต้หัวข้อ 3.6.1.4.3 กำหนดรายละเอียดของคำสั่งเฉพาะสำหรับปัญญาประดิษฐ์ (AI Prompt) เพื่อใช้สำหรับการส่งข้อความแจ้งเตือนดังกล่าวไปยังผู้ใช้เพื่อให้ผู้ใช้ดำเนินการเปลี่ยนรหัสผ่านและเก็บบันทึกรายละเอียดสำหรับวัดผลตามวัตถุประสงค์ของการวิจัย แสดงดังภาพที่ 3-12



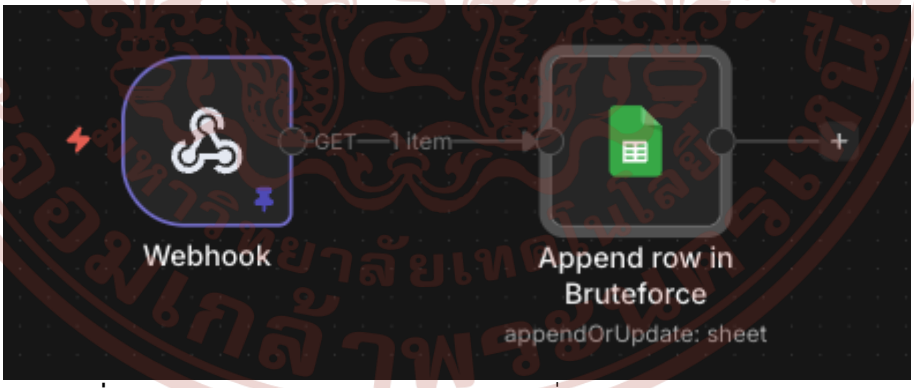
ภาพที่ 3-12 ผลลัพธ์ข้อความแจ้งเตือนผู้ใช้ในการจำลองการโจมตี Bruteforce

ค) สร้างระบบรายงานการถูกโจมตีเป็นเว็บไซต์ที่ให้ผู้ใช้ดำเนินการเปลี่ยนรหัสผ่านทันทีหลังได้รับการแจ้งเตือน Bruteforce แสดงดังภาพที่ 3-13 การกระทำนี้ถูกบันทึกโดย Wazuh Agent และถูกส่งไปยัง Wazuh Server เพื่อดำเนินการต่อไป



ภาพที่ 3-13 หน้าเปลี่ยนรหัสผ่านบนระบบรายงาน (Report System)

ง) สร้าง Workflow ใน n8n ในการรับการแจ้งเตือน (Raw JSON) จาก Wazuh Server ผ่าน Webhook เมื่อผู้ใช้กดปุ่มเปลี่ยนรหัสผ่านในระบบรายงานการถูกโจมตี ระบบจะบันทึกเวลาที่ผู้ใช้ดำเนินการนี้ลงในฐานข้อมูล Google Sheet ทันที ข้อมูลเวลานี้ใช้คำนวณ "เวลาตอบสนองของผู้ใช้" และ “อัตราการตอบสนองที่ถูกต้อง” เพื่อวัดว่าผู้ใช้เปลี่ยนรหัสผ่านได้ทันภายใน 90 วินาทีตามเกณฑ์ที่กำหนดหรือไม่ แสดงดังภาพที่ 3-14



ภาพที่ 3-14 Workflow สำหรับบันทึกการเปลี่ยนรหัสผ่านของ Bruteforce

3.6.2 D: Do (การลงมือทำและการทดลอง) เป็นขั้นตอนการพัฒนาและติดตั้งระบบตามแผนที่วางไว้รวมถึงการดำเนินการทดลองจำลองภัยคุกคามจริง มีขั้นตอนดังนี้

3.6.2.1 การติดตั้งและกำหนดค่าฝั่ง Agent (User PC) สามารถทำได้ดังนี้

3.6.2.1.1 ติดตั้ง Wazuh Agent โดยดาวน์โหลดจากหน้าเว็บของ Wazuh โดยตรง ขั้นตอนนี้คือการติดตั้งโปรแกรมหลัก (Wazuh Agent) บนเครื่องคอมพิวเตอร์ของผู้ใช้เพื่อ

ทำหน้าที่เก็บบันทึกเหตุการณ์ของระบบการเข้าเว็บไซต์ต่างๆ เช่น การเข้าถึงเว็บไซต์และส่งบันทึกเหตุการณ์ของระบบดังกล่าวไปยัง Wazuh Server สำหรับการวิเคราะห์ซึ่งเป็นหัวใจสำคัญในการบันทึกพฤติกรรมการตอบสนองของผู้ใช้

3.6.2.1.2 แก้ไขไฟล์ ossec.conf ใน C:\Program Files (x86)\ossec-agent โดยกำหนดค่าให้ Wazuh Agent ส่งบันทึกเหตุการณ์ของระบบที่รวบรวมได้ออกไปยังเครื่องของตัวเอง (127.0.0.1:4544) การตั้งค่านี้จำเป็นต้องการบูรณาการกับซอฟแวร์ชื่อ “Cloudflared” ที่มีความสามารถในการทำให้ Wazuh Agent สามารถเชื่อมต่อกับ Wazuh Server แบบออนไลน์ได้อย่างปลอดภัย แสดงดังภาพที่ 3-15

```
<!--
  Wazuh - Agent - Default configuration for Windows
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>

  <client>
    <server>
      <address>127.0.0.1</address>
      <port>4544</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>windows, windows10</config-profile>
    <crypto_method>aes</crypto_method>
    <notify_time>20</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
  </client>

  <!-- Agent buffer options -->
  <client_buffer>
    <disabled>no</disabled>
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
  </client_buffer>
```

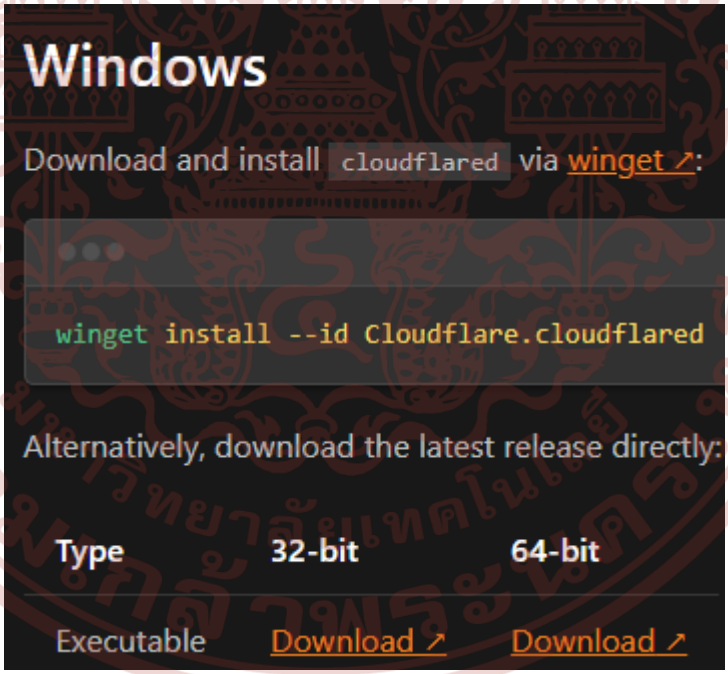
ภาพที่ 3-15 ไฟล์ ossec.conf บน Wazuh Agent ในเครื่องผู้ใช้

3.6.2.1.3 ติดตั้งโมดูล Sysmon เพื่อเก็บข้อมูลติดตามการเข้าใช้งานเว็บไซต์ต่างๆ โดย Sysmon เป็นเครื่องมือเสริมที่ติดตั้งเพื่อให้ Wazuh Agent สามารถเก็บข้อมูลบันทึกเหตุการณ์ของระบบได้อย่างละเอียดขึ้น โดยเฉพาะบันทึกเหตุการณ์ของระบบที่เกี่ยวข้องกับการเข้าใช้งานเว็บไซต์ ซึ่งมีความสำคัญอย่างยิ่งในการติดตามและวิเคราะห์พฤติกรรมการคลิกลิงก์ Phishing จำลองหรือการเข้าถึงระบบรายงานของผู้ใช้เพื่อนำไปใช้คำนวณตัวชี้วัดต่างๆ แสดงดังภาพที่ 3-16

```
<!-- Sysmon -->
<localfile>
  <location>Microsoft-Windows-Sysmon/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
```

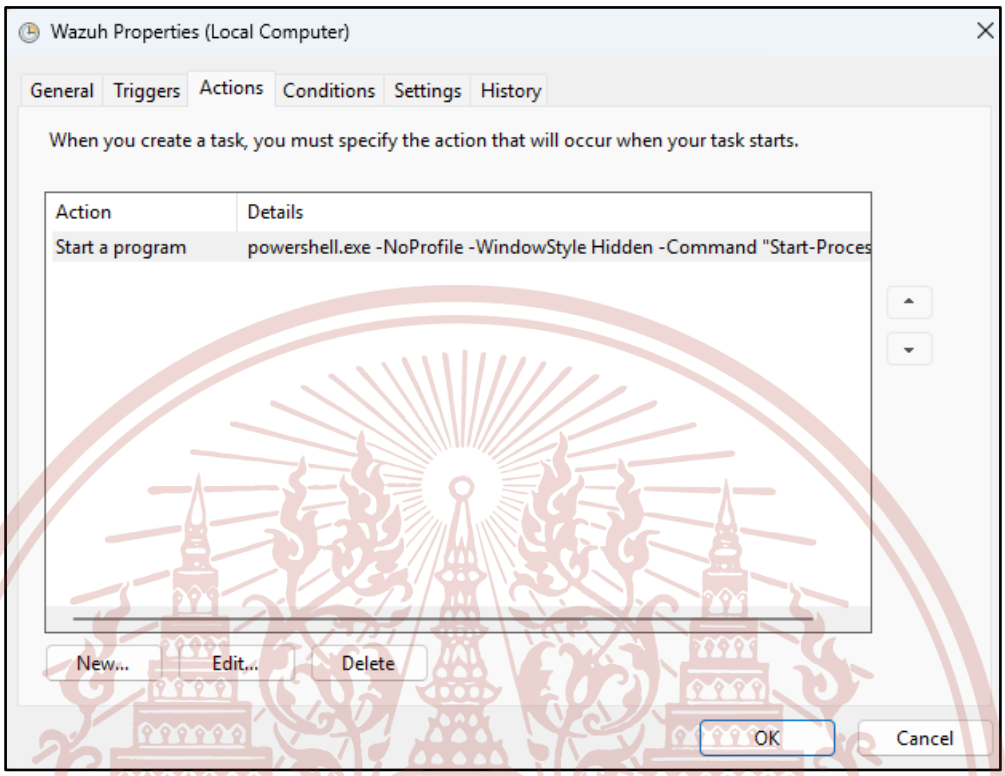
ภาพที่ 3-16 เพิ่ม Sysmon ในไฟล์ ossec.conf บน Wazuh Agent ในเครื่องผู้ใช้

3.6.2.1.4 ติดตั้ง Cloudflared แสดงดังภาพที่ 3-17 เพื่อให้ Wazuh Agent สามารถเชื่อมต่อไปยัง Wazuh Server ได้ โดย Cloudflared เป็นเครื่องมือที่ใช้สร้างท่อส่งข้อมูลพิเศษ (Secure Tunnel) เพื่อให้ Wazuh Agent ที่อยู่บนเครื่องผู้ใช้สามารถเชื่อมต่อและส่งข้อมูลบันทึกเหตุการณ์ของระบบไปยัง Wazuh Server ที่อยู่ภายนอกเครือข่ายได้อย่างปลอดภัย



ภาพที่ 3-17 ติดตั้ง Cloudflared ในเครื่องผู้ใช้

3.6.2.1.5 ตั้งค่า Task schedule บนเครื่องลูกข่ายของผู้ใช้เพื่อให้มั่นใจว่าการเชื่อมต่อที่สร้างด้วย Cloudflared จะทำงานและเชื่อมต่อระหว่าง Wazuh Agent กับ Wazuh Server โดยอัตโนมัติหลังจากเปิดเครื่อง ซึ่งเป็นการรับประกันว่าบันทึกเหตุการณ์ของระบบกิจกรรมทั้งหมดจะถูกส่งไปยัง Server ได้ตลอดเวลา แสดงดังภาพที่ 3-18



ภาพที่ 3-18 ตั้งค่า Task schedule บนเครื่องผู้ใช้

3.6.2.2 การติดตั้งและกำหนดค่าฝั่ง Server/Automation (Wazuh Server, n8n, AI)

3.6.2.2.1 จัดทำฐานข้อมูลเพื่อเก็บข้อมูลในการคำนวณ ใช้ Google Sheet เป็นฐานข้อมูลหลักเพื่อจัดเก็บข้อมูลดิบที่ได้จากการจำลองภัยคุกคามทั้งแบบ Phishing และ Bruteforce เพื่อนำไปคำนวณค่าตัวชี้วัดด้านผู้ใช้งานรวมถึงตัวชี้วัดด้านระบบเพื่อตอบวัตถุประสงค์การวิจัย

3.6.2.2.2 ตั้งค่า Wazuh Server สามารถทำตามขั้นตอนต่อไปนี้

ก) แก้ไขไฟล์ ossec.conf บน Wazuh Server ที่ /var/ossec/etc/ เพื่อให้ระบบสามารถส่งข้อมูลไป n8n ได้ แสดงดังภาพที่ 3-19 การแก้ไขไฟล์ ossec.conf บน Wazuh Server เป็นการกำหนดค่าให้ระบบสามารถส่งการแจ้งเตือนดิบ (Raw JSON) ผ่าน Webhook ไปยังระบบอัตโนมัติ n8n ได้โดยอัตโนมัติเพื่อให้ n8n ทำหน้าที่เป็น Workflow ในการรับข้อมูลและส่งต่อให้ปัญญาประดิษฐ์ประมวลผลในขั้นตอนต่อไป

```
<integration>
  <name>n8n</name>
  <hook_url>https://n8n.cheetahis.me/webhook/wazuh-alerts</hook_url>
  <rule_id>60122</rule_id>
  <alert_format>json</alert_format>
  <level>3</level>
</integration>
```

ภาพที่ 3-19 แก้ไขไฟล์ ossec.conf บน Linux Server

ข) แก้ไขกฎในไฟล์ /var/ossec/etc/rules/local_rules.xml บน Wazuh Server มีวัตถุประสงค์เพื่อกำหนดกฎ (Rules) ให้ Wazuh Server สร้างและส่งการแจ้งเตือนดิบไปยัง Workflow n8n เพื่อเริ่มกระบวนการทำงานอัตโนมัติ โดยกระบวนการดังกล่าวเริ่มต้นเมื่อ Wazuh Agent บนเครื่องผู้ใช้ตรวจจับกิจกรรมที่กำหนดได้ เช่น การคลิกลิงก์ Phishing บนอีเมล Phishing จำลองหรือคลิกเปลี่ยนรหัสผ่านบนระบบรายงาน แสดงดังภาพที่ 3-20

```
<group name="sysmon_test,">

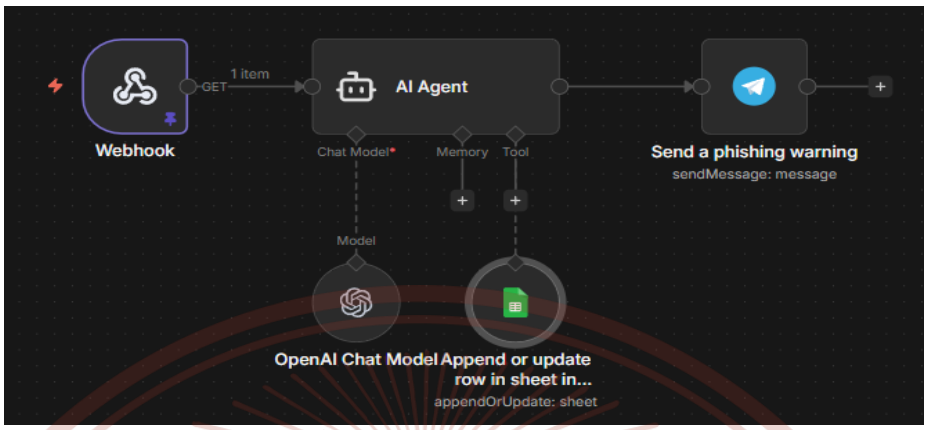
  <rule id="100022" level="5">
    <field name="win.system.eventID">^22$</field>
    <field name="win.eventdata.image" type="pcre2">chrome\.exe$</field>
    <description>Chrome Visited: $(win.eventdata.queryName)</description>
  </rule>
```

ภาพที่ 3-20 แก้ไขไฟล์ local_rules.xml บน Wazuh Server

3.6.2.2.3 การสร้าง n8n Workflow ประกอบด้วย n8n Workflow สำหรับการโจมตีจำลองแบบ Phishing จำนวน 2 Workflows และแบบ Bruteforce จำนวน 2 Workflows มีรายละเอียดดังนี้

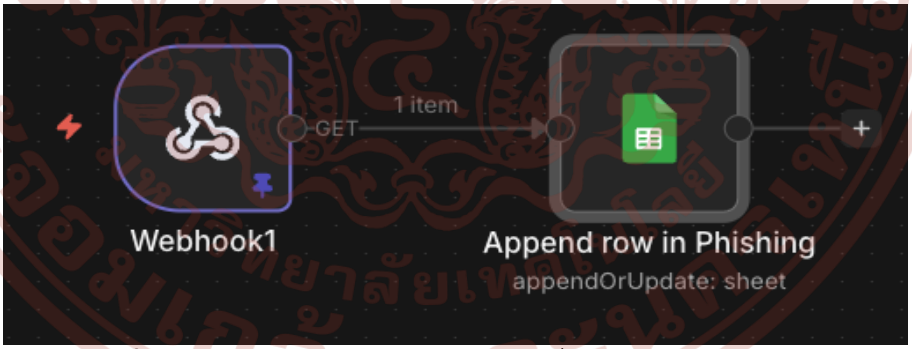
ก) n8n Workflow สำหรับการโจมตีจำลองแบบ Phishing

(1) Workflow ที่ใช้สำหรับรับข้อมูลการแจ้งเตือนดิบจาก Wazuh Server เพื่อแจ้งผู้ใช้ให้เปลี่ยนรหัสผ่านในกรณีที่ผู้ใช้เผลอคลิกลิงก์ Phishing ในอีเมล Phishing จำลอง โดยขั้นตอนของการทำงานของ Workflow นี้เริ่มจาก Workflow ได้รับการแจ้งเตือนเข้ามาผ่าน Webhook จากนั้นระบบจะบันทึกเวลากิจกรรมลงใน Google Sheet และดำเนินการแปลผลการแจ้งเตือนทางเทคนิคให้เป็นข้อความที่เข้าใจง่ายพร้อมคำแนะนำในการเปลี่ยนรหัสผ่านบนระบบรายงานการถูกโจมตี ซึ่งข้อความแจ้งเตือนจะแตกต่างกันในแต่ละครั้ง อันเป็นผลมาจากการสร้างใหม่จากชุดคำสั่ง (Prompt) ที่กำหนดไว้ในหัวข้อ Phishing ที่อยู่ภายใต้หัวข้อ 3.6.1.4.3 กำหนดรายละเอียดของคำสั่งเฉพาะสำหรับปัญญาประดิษฐ์ก่อนส่งแจ้งเตือนไปยังผู้ใช้ผ่าน Telegram แสดงดังภาพที่ 3-21



ภาพที่ 3-21 Workflow สำหรับรับการแจ้งเตือนเมื่อผู้ใช้กดลิงก์ Phishing

(2) Workflow ที่ใช้สำหรับรับข้อมูลการแจ้งเตือนดิบจาก Wazuh Server เพื่อบันทึกเวลาการเปลี่ยนรหัสผ่านการโจมตีแบบ Phishing โดยขั้นตอนของการทำงานของ Workflow นี้เริ่มหลังจาก Wazuh Server ส่งการแจ้งเตือนดิบมายัง Workflow n8n ผ่าน Webhook เมื่อระบบได้รับการแจ้งเตือนดิบจาก Wazuh Server เข้ามา ระบบจะบันทึกเวลาการเปลี่ยนรหัสผ่านลงใน Google Sheet และจบกระบวนการทำงานโดยไม่มีการแจ้งเตือนไปยังผู้ใช้ แสดงดังภาพที่ 3-22

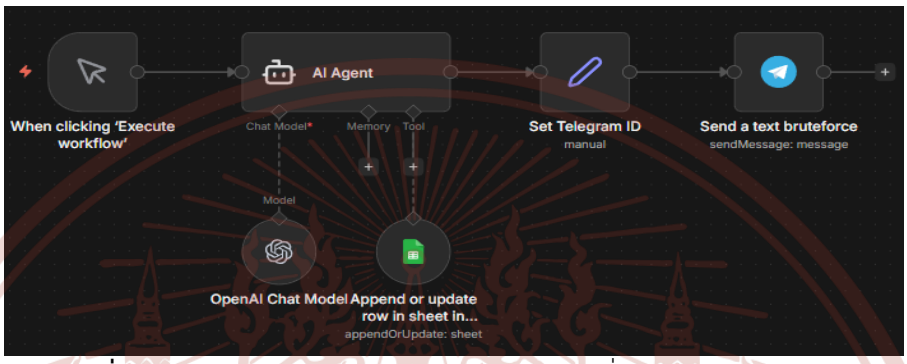


ภาพที่ 3-22 Workflow บันทึกเวลาการเปลี่ยนรหัสผ่านของ Phishing

ข) n8n Workflow สำหรับการโจมตีจำลองแบบ BruteForce

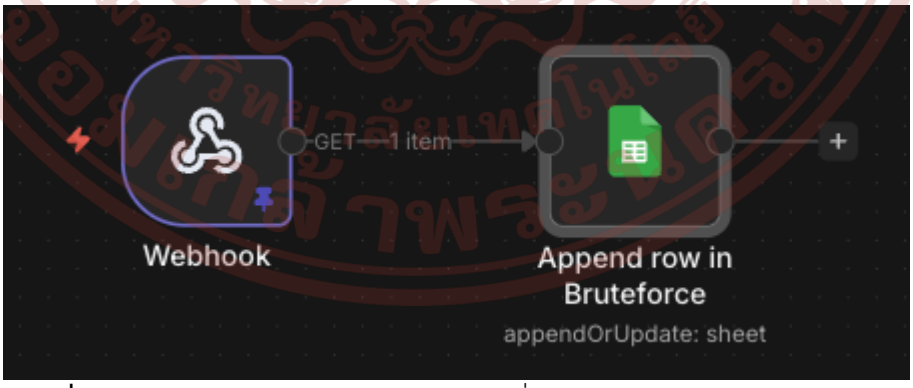
(1) Workflow ที่ใช้สำหรับส่งการแจ้งเตือนจำลอง Bruteforce ไปยังผู้ใช้เพื่อให้ผู้ใช้เปลี่ยนรหัสผ่าน โดยขั้นตอนของการทำงานของ Workflow นี้เริ่มจากผู้วิจัยกดปุ่มเริ่มส่งข้อความแจ้งเตือน จากนั้น Workflow จะสั่งงานปัญญาประดิษฐ์ให้สร้างข้อความแจ้งเตือนที่เข้าใจง่ายและกระชับพร้อมคำแนะนำและลิงก์ในการเปลี่ยนรหัสผ่านบนระบบรายงานการถูกโจมตีเพื่อกระตุ้นให้ผู้ใช้เปลี่ยนรหัสผ่านทันที ซึ่งข้อความแจ้งเตือนจะแตกต่างกันใน

แต่ละครั้งอันเป็นผลมาจากการสร้างใหม่จากชุดคำสั่ง (Prompt) ที่กำหนดไว้ในหัวข้อ Bruteforce ที่อยู่ภายใต้หัวข้อ 3.6.1.4.3 กำหนดรายละเอียดของคำสั่งเฉพาะสำหรับปัญญาประดิษฐ์ ก่อนส่งแจ้งเตือนไปยังผู้ใช้ผ่าน Telegram แสดงดังภาพที่ 3-23



ภาพที่ 3-23 Workflow สำหรับรับการแจ้งเตือนเมื่อผู้ใช้กดลิงก์ Phishing

(2) Workflow ที่ใช้สำหรับรับข้อมูลการแจ้งเตือนดิบจาก Wazuh Server เพื่อบันทึกเวลาการเปลี่ยนรหัสผ่านการโจมตีแบบ Bruteforce โดยขั้นตอนของการทำงานของ Workflow นี้เริ่มหลังจาก Wazuh Server ส่งการแจ้งเตือนดิบมายัง Workflow n8n ผ่าน Webhook เมื่อระบบได้รับการแจ้งเตือนดิบจาก Wazuh Server เข้ามา ระบบจะบันทึกเวลาการเปลี่ยนรหัสผ่านลงใน Google Sheet และจบกระบวนการทำงานโดยไม่มีการแจ้งเตือนไปยังผู้ใช้ แสดงดังภาพที่ 3-24



ภาพที่ 3-24 Workflow สำหรับบันทึกการเปลี่ยนรหัสผ่านของ Bruteforce

3.6.2.3 อบรมกลุ่มตัวอย่างเกี่ยวกับความเสี่ยงของภัยคุกคาม และขั้นตอนการตอบสนองที่ถูกต้องเมื่อได้รับแจ้งเตือนจากระบบเพื่อตอบสนองต่อภัยคุกคามได้อย่างทันท่วงที ประสิทธิภาพของการอบรมนี้จะถูกวัดผลโดย Security Awareness Score (จากการเปรียบเทียบผล Pre-test และ Post-test) โดยมีเป้าหมายความสำเร็จคือ คะแนนสอบหลังการทดลอง (Post-test) ต้อง มากกว่า 70% แสดงดังภาพที่ 3-25 และ 3-26



ภาพที่ 3-25 ตัวอย่างวิดีโอการอบรม



ภาพที่ 3-26 คู่มือการตอบสนองต่อภัยคุกคาม

3.6.2.4 การดำเนินการโจมตีจำลอง (Simulated Attacks) จำนวนอย่างละ 125 ครั้ง ได้แก่ Phishing และ Bruteforce เป็นขั้นตอนการทดลองและเก็บข้อมูลในช่วง D: Do ของ วัฏจักร PDCA มีวัตถุประสงค์เพื่อจำลองสถานการณ์ภัยคุกคามจริงเพื่อกระตุ้นให้ระบบ Wazuh IDS สร้างการแจ้งเตือนทางเทคนิคและให้การแจ้งเตือนดังกล่าวถูกส่งต่อผ่าน Workflow Engine (n8n) ไปยังผู้ใช้ เมื่อผู้ใช้ได้รับแจ้งเตือนและดำเนินการตอบสนองตามคำแนะนำ (เปลี่ยนรหัสผ่าน) ระบบจะบันทึกพฤติกรรมและเวลาที่ใช้ในการตอบสนองนั้นลงในฐานข้อมูลเพื่อนำไปคำนวณตัวชี้วัดประสิทธิภาพด้านผู้ใช้งานหลักๆ เช่น เวลาตอบสนองของผู้ใช้ และอัตราการตอบสนองที่ถูกต้องตามที่กำหนดไว้

3.6.3 ในขั้นตอน C: Check (การตรวจสอบและวิเคราะห์ผล) ข้อมูลที่ถูกรวบรวมจากขั้นตอนการทดลอง (D: Do) จะถูกนำมาวิเคราะห์ทั้งในเชิงปริมาณ (Quantitative) และเชิงคุณภาพ (Qualitative) ตามตัวชี้วัดที่กำหนดไว้ดังนี้

3.6.3.1 การวัดผลประสิทธิภาพด้านระบบในขั้นตอน C: Check ประกอบด้วยสองส่วนหลัก ส่วนแรกคือการวัดผลประสิทธิภาพทางเทคนิคตามเกณฑ์ Precision, Recall, F1-score และ Detection Time โดยใช้ค่าเหล่านี้เพื่อยืนยันความแม่นยำและความสามารถ ในการตรวจจับภัยคุกคามของระบบ Wazuh IDS n8n และ AI กล่าวคือ Precision และ Recall ถูกใช้เพื่อประเมินความสามารถของระบบในการจำแนกลิงก์ได้อย่างถูกต้องพร้อมทั้งลดอัตราการแจ้งเตือนที่ผิดพลาด (False Positives) และอัตราการตรวจไม่พบ (False Negatives) ตามลำดับ นอกจากนี้ยังใช้ค่าเฉลี่ยแบบ Harmonic Mean ของ Precision และ Recall (F1-score) เพื่อให้ได้ค่าความแม่นยำที่ครอบคลุม ในขณะที่ Detection Time มีวัตถุประสงค์เพื่อประเมินความ สามารถในการสร้างการแจ้งเตือนที่รวดเร็วเพื่อส่งต่อข้อมูลไปยังส่วนประมวลผลอัตโนมัติได้ทันท่วงที ส่วนที่สองคือการวัดผลกระทบต่อระบบ (System Performance) โดยวัดเปอร์เซ็นต์การใช้ทรัพยากรเครื่อง (CPU และ Memory/RAM) ของเครื่อง Wazuh Server และ Agent ในช่วงที่มีการโจมตีจำลอง ซึ่งมีวัตถุประสงค์เพื่อประเมินว่าระบบที่พัฒนาขึ้นสร้างภาระ (Overhead) มากเกินไปจนส่งผลกระทบต่อการใช้งานปกติของเครื่องคอมพิวเตอร์และเครื่อง Server หรือไม่

3.6.3.2 การวัดผลประสิทธิภาพของผู้ใช้ในขั้นตอน C: Check มีวัตถุประสงค์เพื่อยืนยันว่าการบูรณาการระบบอัตโนมัติและปัญญาประดิษฐ์ (n8n/AI) สามารถช่วยให้ผู้ใช้งานทั่วไปตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพจริง โดยมุ่งเน้นการวัดผลตามเกณฑ์หลักสองประการ

3.6.3.2.1 วัดผลการตอบสนองของผู้ใช้ที่ถูกต้องและทันเวลา (Correct Response Rate และ User Response Time) ซึ่งมีความสำคัญในการยืนยันว่าผู้ใช้งานมี

ความตระหนักรู้ด้านความปลอดภัย (Security Awareness) และสามารถดำเนินการตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและถูกต้อง

3.6.3.2.2 ประเมินความรู้ความเข้าใจ (Security Awareness Score) โดยเริ่มจากการวัดระดับความรู้ความเข้าใจด้านความปลอดภัยด้วยแบบทดสอบก่อนการวิจัย (Pre-test) และนำผลที่ได้มาเปรียบเทียบกับแบบทดสอบหลังการทดลอง (Post-test) ในภายหลัง การเปรียบเทียบนี้มีวัตถุประสงค์เพื่อประเมินผลลัพธ์การพัฒนาความตระหนักรู้ด้านความปลอดภัยด้านเทคโนโลยีสารสนเทศและความปลอดภัยไซเบอร์ของผู้ใช้ โดยเป้าหมายความสำเร็จของคะแนนสอบหลังการทดลองโดยรวมถูกกำหนดไว้ที่มากกว่า 70% เพื่อยืนยันว่าผู้ใช้งานมีความรู้ความเข้าใจเกี่ยวกับประเภทภัยคุกคาม ความหมายของการแจ้งเตือน และขั้นตอนการตอบสนองที่ถูกต้องเพิ่มขึ้น

3.6.3.3 การวิเคราะห์ผลแบบเชิงคุณภาพ (Qualitative Analysis) มีวัตถุประสงค์เพื่อทำความเข้าใจประสบการณ์ของผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญที่มีต่อระบบแจ้งเตือนที่แปลผลด้วย AI ซึ่งเป็นส่วนหนึ่งของขั้นตอน C: Check ในวัฏจักร PDCA โดยผู้วิจัยได้ดำเนินการรวบรวมและวิเคราะห์ผลตอบรับเชิงคำพูด (Pain Points) เพื่อสอบถามความคิดเห็นแบบเปิดจากผู้ใช้งาน ข้อมูลเชิงคุณภาพที่ได้จากการวิเคราะห์นี้มีความสำคัญอย่างยิ่ง เนื่องจากจะถูกนำไปใช้ในการปรับปรุงระบบในขั้นตอน A: Act (การปรับปรุงและการนำไปใช้) เช่น การปรับปรุงแก้ไข (Fine-tune) คำสั่ง (Prompt) ของ AI ซึ่งส่งผลโดยตรงให้ข้อความแจ้งเตือนที่ส่งให้ผู้ใช้มีความเข้าใจง่าย ชัดเจนมากขึ้น รวมถึงช่วยลดความสับสนของข้อความอีกด้วย

3.6.4 A: Act (การปรับปรุงและการนำไปใช้)

3.6.4.1 นำข้อค้นพบจากขั้นตอน C: Check มาใช้ในการปรับปรุงวัฏจักร PDCA เพื่อแก้ไขปัญหาที่ตรวจพบและเพิ่มประสิทธิภาพการตอบสนองของผู้ใช้ให้ดียิ่งขึ้น เช่น การปรับปรุงแก้ไขกฎการแจ้งเตือน (Rule) บน Wazuh Server การปรับปรุงแก้ไข (Fine-tune) คำสั่ง (Prompt) ของ AI ใน Workflow n8n และการปรับปรุงขั้นตอนการทำงานของ Workflow n8n โดยมีการปรับปรุงแก้ไขตามผลตอบรับจากผู้ใช้ ซึ่งสามารถอธิบายได้ว่า การนำข้อค้นพบจากขั้นตอน Check มาใช้ในการปรับปรุง ผู้วิจัยได้ดำเนินการปรับปรุงหลักสามส่วน โดยเริ่มจากการปรับปรุงคำสั่ง (Fine-tune Prompt) ของ AI ใน n8n ให้ข้อความแจ้งเตือนมีรูปแบบและโทนที่เข้าใจง่ายขึ้น และลดลักษณะของข้อความที่เหมือนสแปมลงตามผลตอบรับของผู้ใช้เพื่อลดความตื่นตระหนกและความสับสนที่เกิดขึ้น ต่อมาคือการปรับปรุง UI/UX ของข้อความแจ้งเตือนด้วยการเพิ่มองค์ประกอบทางสายตา เช่น การใช้สีหรือไอคอนที่ระบุระดับความรุนแรงของภัยคุกคาม (เช่น สีแดงสำหรับ "ด่วนมาก") เพื่อช่วยให้รับรู้ถึงความสำคัญและดำเนินการตอบสนองได้เร็วขึ้น และส่วนสุดท้ายคือการประเมินและปรับปรุงประสิทธิภาพของระบบรายงานการถูกโจมตี ซึ่งมุ่งแก้ไขปัญหาเวลาหน่วงโดยรวมของระบบ โดย

การปรับเพิ่ม Ram ของ VM ที่ใช้เปิดระบบรายงาน ซึ่งมีความสำคัญต่อการแก้ไขปัญหาความหน่วงของระบบรายงานที่ส่งผลกระทบต่อเวลาตอบสนองของผู้ใช้ (User Response Time) โดยตรง

3.6.4.2 การปรับปรุงที่เกิดขึ้นถูกนำไปประยุกต์ใช้ในการทดลองอย่างสม่ำเสมอ ซึ่งเป็นการยืนยันว่ากระบวนการพัฒนาประสิทธิภาพการตอบสนองต่อภัยคุกคามไซเบอร์ผ่านการบูรณาการระบบและวัฏจักร PDCA นั้นสามารถดำเนินไปได้อย่างยั่งยืนและต่อเนื่อง

3.7 มาตรการความปลอดภัยและแผนการรับมือ (Rollback)

การแจ้งผู้เข้าร่วมว่ามีการทดสอบเพื่อให้ผู้เข้าร่วมเตรียมตัวสำหรับการตอบสนองต่อภัยคุกคามของการวิจัยและเข้าใจแผน Rollback เนื้อหานี้ถูกกำหนดขึ้นเพื่อเป็น "เบรกฉุกเฉิน" ในการดำเนินการวิจัยเพื่อให้มั่นใจว่าหากเกิดข้อผิดพลาดร้ายแรง ระบบสามารถถูกยุติและคืนค่าสภาพเดิมได้อย่างรวดเร็ว โดยแบ่งออกเป็น 2 กรณี ได้แก่ ปัญหาที่เกิดจากผลกระทบต่อเครื่องคอมพิวเตอร์ (Device Impact) เช่น Wazuh Agent กินทรัพยากรเครื่องสูงผิดปกติและปัญหาที่เกิดจากระบบแจ้งเตือนรวน (Notification Spam/Error) เช่น ผู้ใช้ได้รับข้อความแจ้งเตือนรัวๆ หรือ AI แปลความหมายผิด โดยแต่ละกรณีมีขั้นตอนการรับมือและการยกเลิกการทำงานของระบบที่ชัดเจนเพื่อแก้ไขปัญหาได้ทันท่วงที แสดงดังตารางที่ 3-6

ตารางที่ 3-6 มาตรการความปลอดภัยและแผนการรับมือ

ลำดับ	กรณีปัญหา (Scenario)	ปัญหา (Issue)	มาตรการ Rollback และการรับมือ
	ผลกระทบต่อเครื่องคอมพิวเตอร์ (Device Impact)	Wazuh Agent กินทรัพยากรเครื่องสูงผิดปกติ (High CPU/RAM usage) จนผู้ใช้ทำงานไม่ได้	1. กดปุ่ม Windows และค้นหา "add or remove programs" 2. ใช้ช่องค้นหา พิมพ์ "Wazuh" 3. คลิกที่จุดไข่ปลา 3 จุดที่ "Wazuh Agent" จากนั้นเลือก "Uninstall" 4. รอโปรแกรมถอนการติดตั้ง 5. รีสตาร์ทเครื่อง

ตารางที่ 3-6 (ต่อ)

	ระบบแจ้งเตือนรวน (Notification Spam/Error)	ผู้ใช้ได้รับข้อความแจ้งเตือนรัวๆ เป็นร้อยข้อความ (Notification Storm) หรือ AI แปลความหมายผิดจนเกิดความตื่นตระหนก	1. กดหยุด Workflow บน n8n Server ทันทีเพื่อหยุดการส่งข้อความชั่วคราว 2. แจ้งเตือนผู้ใช้: ส่งข้อความแจ้งผู้ใช้ผ่าน Line กลุ่ม 3. แก้ไขระบบให้ใช้งานได้ตามปกติ

3.8 แผนผังขั้นตอนการดำเนินงาน (Operation Plan)

แผนผังขั้นตอนการดำเนินงานคือ ระยะเวลาดำเนินงานตลอดระยะเวลา 6 เดือน (พฤศจิกายน 2568 – เมษายน 2569) ที่เป็นการจัดลำดับกิจกรรมหลักและกิจกรรมย่อยของการวิจัยตามวัฏจักรอย่างเป็นขั้นตอน โดยเริ่มต้นตั้งแต่การวางแผนระบบ (Plan) ไปจนถึงการพัฒนาและติดตั้งระบบต้นแบบ (Do) การวัดผลและประสิทธิภาพทั้งด้านเทคนิคและผู้ใช้ (Check) รวมถึงการปรับปรุงระบบและการเข้าสู่วัฏจักรใหม่ (Act) แสดงดังตารางที่ 3-7 ซึ่งแสดงถึงแผนผังขั้นตอนการดำเนินงานวิจัย (Operation Plan) ซึ่งใช้การเปรียบเทียบความหนักเบาของจำนวนดาวเพื่อบ่งบอกถึงช่วงเวลาและความเข้มข้นของการ ทำงานในแต่ละเดือนกิจกรรมหลักครอบคลุมตั้งแต่การทบทวนวรรณกรรมและการวางแผนระบบ PDCA ซึ่งตารางนี้ช่วยให้สามารถติดตามความคืบหน้าและบริหารจัดการทรัพยากรเพื่อให้งานวิจัยเสร็จสิ้นตามกรอบเวลาที่กำหนดไว้ได้อย่างชัดเจน นอกจากนี้ ภายในแผนการดำเนินงานดังกล่าวแสดงถึงการเปรียบเทียบความหนักเบา ของจำนวนดาว มีรายละเอียดดังนี้

- ★★★ (3 ดาว): หมายถึงกิจกรรมหลัก ที่ใช้เวลาส่วนใหญ่ของเดือนในการดำเนินการ
- ★★ (2 ดาว): หมายถึงงานยังคงดำเนินการอยู่ แต่ใช้เวลาดำเนินการ ประมาณครึ่งหนึ่งของเดือน
- ★ (1 ดาว): หมายถึงงานอยู่ในช่วง เริ่มต้น หรือ สิ้นสุด หรือเป็นกิจกรรมที่ใช้เวลาน้อยที่สุดในเดือนนั้น

ตารางที่ 3-7 แผนผังขั้นตอนการดำเนินงาน

ลำดับ	กิจกรรมหลักและกิจกรรมย่อย	พ.ย. 2568	ธ.ค. 2568	ม.ค. 2569	ก.พ. 2569	มี.ค. 2569	เม.ย. 2569
10.1	การทบทวนวรรณกรรมและการออกแบบระบบ	★★					
10.2	การกำหนดกลุ่มตัวอย่าง		★				
10.3	การจัดเตรียมเครื่องมือวัดผลและ Pre-test /Post-test		★★				
10.4	กำหนดวัตถุประสงค์การทดสอบ		★★				
10.5	กำหนดมาตรการความปลอดภัยและ Rollback		★				
10.6	พัฒนาและติดตั้งระบบต้นแบบ			★★			
10.7	พัฒนา n8n Automation Workflow			★★			
10.8	การให้ผู้เข้าร่วมทดลองใช้ระบบ ในการใช้งานประจำวัน			★	★★		
10.9	การโจมตีจำลองและการบันทึกข้อมูล			★	★★		
10.10	วัดผลประสิทธิภาพ ระบบ				★		
10.11	วัดผลกระทบต่อระบบ					★	

ตารางที่ 3-7 (ต่อ)

10.12	วัดผลประสิทธิภาพผู้ใช้					★	
10.13	ประเมินความรู้ความเข้าใจ (Post-test)					★★	
10.14	วิเคราะห์ผลแบบเชิงคุณภาพ					★★	
10.15	การปรับปรุงระบบและนำข้อค้นพบจาก Check มาปรับจูนกฎต่างๆ					★★	
10.16	การเข้าสู่วัฏจักรใหม่โดยนำการปรับปรุงไปใช้ในการทดลองรอบต่อไป					★	★★

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

บทที่ 4
ผลการวิจัยและอภิปรายผล

4.1 ผลการประเมินประสิทธิภาพด้านระบบ (System Metrics)

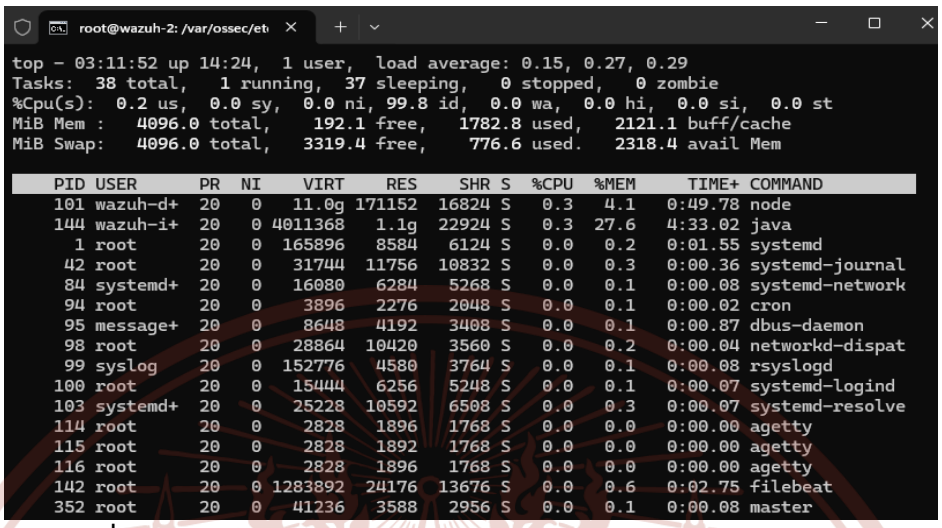
ผลการทดลองวัดประสิทธิภาพทางเทคนิคของระบบตรวจจับภัยคุกคาม Wazuh IDS และระบบอัตโนมัติ (n8n/AI) เพื่อยืนยันความสามารถในการทำงานที่เชื่อถือได้มีดังนี้

4.1.1 ความแม่นยำในการตรวจจับ (Detection Accuracy) สามารถวัดผลประสิทธิภาพระบบได้จากเกณฑ์ที่กำหนด ได้แก่ Precision, Recall, และ F1-score จากการทดลองใช้งานระบบจริงตามขั้นตอน D: Do (การลงมือทำ) ผลการตรวจสอบและวิเคราะห์ประสิทธิภาพของระบบบูรณาการมีประสิทธิภาพทางเทคนิคสูง โดยค่าความแม่นยำ (Precision) อยู่ที่ 100% (1.0) เนื่องจากเป็นการส่งภัยคุกคามโดยผู้วิจัยเอง จึงไม่มีการแจ้งเตือนที่ผิดพลาด (False Positive) ขณะที่ค่าความรำลึก (Recall) อยู่ที่ 100% (1.0) แสดงว่าระบบสามารถดักจับและส่งแจ้งเตือนได้ครบทุกเหตุการณ์โดยไม่มีการตรวจไม่พบ (False Negative) และค่า F1-Score ก็อยู่ที่ 1.0 ซึ่งคำนวณจากค่า Precision และ Recall ที่สมบูรณ์ดังกล่าว

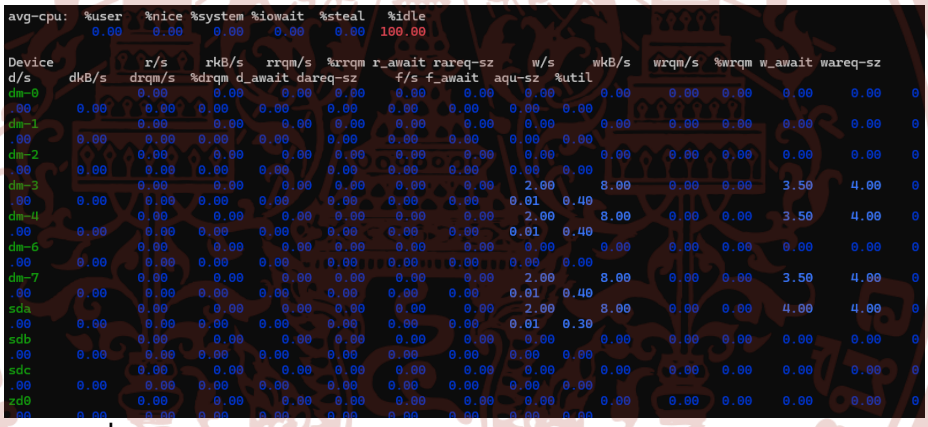
4.1.2 เวลาในการตรวจจับเฉลี่ย (Avg. Detection Time) ของระบบบูรณาการอยู่ที่ประมาณ 5.31 วินาที โดยสัดส่วนความเร็วในการตรวจจับอยู่ในช่วง 3-4 วินาที คิดเป็น 57.6% ของรายการทั้งหมด

4.1.3 การวัดผลกระทบต่อทรัพยากรระบบ (System Performance) เช่น CPU, Memory I/O ของ Wazuh Server และ Agents โดยวัดผลทั้งในสถานการณ์ปกติและช่วงโหลดสูงสุด (Peak Load) ซึ่งผลการทดสอบแสดงให้เห็นว่า มีการใช้ทรัพยากรไม่สูงจนเกินไป

4.1.3.1 การวัดผลกระทบต่อทรัพยากรระบบ Server และ Agent ในสถานการณ์ปกติแสดงดังภาพที่ 4-1 และภาพที่ 4-2

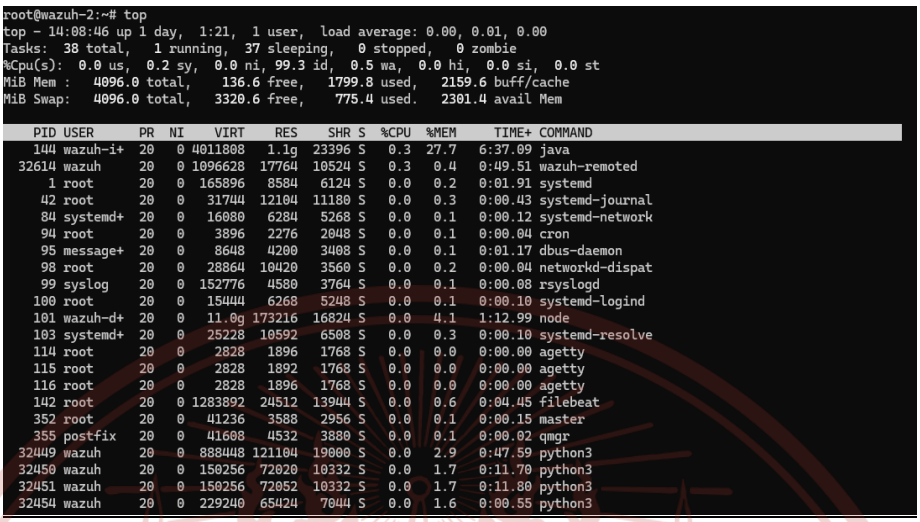


ภาพที่ 4-1 วัดผลกระทบของ Server ต่อทรัพยากรระบบในสถานการณ์ปกติ



ภาพที่ 4-2 วัดผลกระทบของ Agent ต่อทรัพยากรระบบในสถานการณ์ปกติ

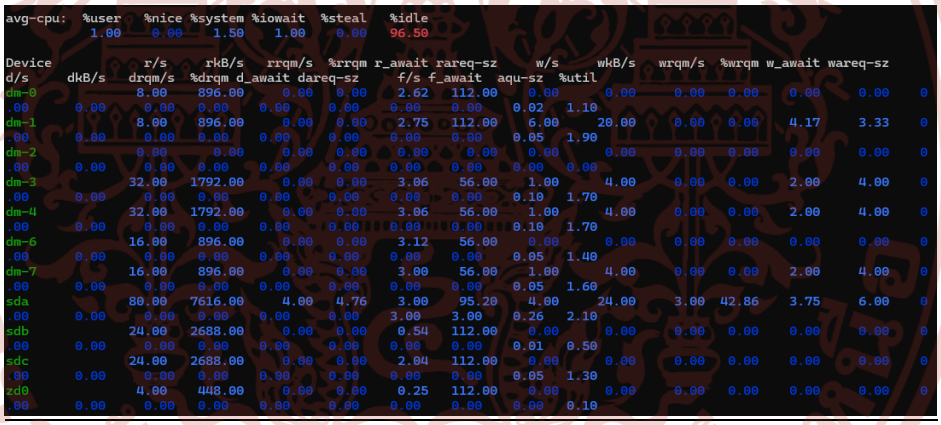
4.1.3.2 การวัดผลกระทบต่อทรัพยากรระบบในสถานการณ์โหลดสูงแสดงดังภาพที่ 4-3 และภาพที่ 4-4



```
root@wazuh-2:~# top
top - 14:08:46 up 1 day,  1:21,  1 user,  load average: 0.00, 0.01, 0.00
Tasks:  38 total,   1 running,  37 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.2 sy,  0.0 ni, 99.3 id,  0.5 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   4096.0 total,    136.6 free,   1799.8 used,   2159.6 buff/cache
MiB Swap:   4096.0 total,   3320.6 free,    775.4 used.   2301.4 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    144 wazuh-i+  20   0 4011808   1.1g  23396 S   0.3  27.7   6:37.09 java
  32614 wazuh     20   0 1096628  17764  10524 S   0.3   0.4   0:49.51 wazuh-remoted
      1 root      20   0  165896   8584   6124 S   0.0   0.2   0:01.91 systemd
     42 root      20   0   31744  12104  11180 S   0.0   0.3   0:00.43 systemd-journal
     84 systemd+  20   0   16080   6284   5268 S   0.0   0.1   0:00.12 systemd-network
     94 root      20   0    3896   2276   2048 S   0.0   0.1   0:00.04 cron
     95 message+  20   0    8648   4200   3408 S   0.0   0.1   0:01.17 dbus-daemon
     98 root      20   0   28864  10420   3560 S   0.0   0.2   0:00.04 networkd-dispat
     99 syslog    20   0  152776   4580   3764 S   0.0   0.1   0:00.08 rsyslogd
    100 root      20   0   15444   6268   5248 S   0.0   0.1   0:00.10 systemd-logind
    101 wazuh-d+  20   0   11.0g 173216  16824 S   0.0   4.1   1:12.99 node
    103 systemd+  20   0   25228  10592   6508 S   0.0   0.3   0:00.10 systemd-resolve
    114 root      20   0    2828   1896   1768 S   0.0   0.0   0:00.00 agetty
    115 root      20   0    2828   1892   1768 S   0.0   0.0   0:00.00 agetty
    116 root      20   0    2828   1896   1768 S   0.0   0.0   0:00.00 agetty
    142 root      20   0 1283892  24512  13944 S   0.0   0.6   0:04.45 filebeat
    352 root      20   0   41236   3588   2956 S   0.0   0.1   0:00.15 master
    355 postfix   20   0   41608   4532   3880 S   0.0   0.1   0:00.02 qmgr
  32449 wazuh     20   0  888448 121104  19000 S   0.0   2.9   0:47.59 python3
  32450 wazuh     20   0  150256  72020  10332 S   0.0   1.7   0:11.70 python3
  32451 wazuh     20   0  150256  72052  10332 S   0.0   1.7   0:11.80 python3
  32454 wazuh     20   0  229240  65424   7044 S   0.0   1.6   0:00.55 python3
```

ภาพที่ 4-3 วัดผลกระทบของ Server ต่อทรัพยากรระบบในสถานการณ์โหลดสูง



```
avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           1.00    0.00    1.50    1.00    0.00   96.50

Device            r/s     rkB/s   rrqm/s  %rrqm r_await rareq-sz     w/s     wkB/s   wrqm/s  %wrqm w_await wareq-sz
d/s     dkB/s   drqm/s  %drqm d_await dareq-sz     f/s f_await  aqu-sz  %util
dm-0             8.00    896.00     0.00   0.00    2.62   112.00    0.00      0.00     0.00   0.00    0.00     0.00    0
.00      0.00     0.00   0.00    0.00    0.00    0.00    0.00    0.02   1.10
dm-1             8.00    896.00     0.00   0.00    2.75   112.00    6.00     20.00     0.00   0.00    4.17     3.33    0
.00      0.00     0.00   0.00    0.00    0.00    0.00    0.00    0.05   1.90
dm-2             0.00      0.00     0.00   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0
.00      0.00     0.00   0.00    0.00    0.00    0.00    0.00    0.00   0.00
dm-3            32.00   1792.00     0.00   0.00    3.06    56.00    1.00      4.00     0.00   0.00    2.00     4.00    0
.00      0.00     0.00   0.00    0.00    0.00    0.00    0.00    0.10   1.70
dm-4            32.00   1792.00     0.00   0.00    3.06    56.00    1.00      4.00     0.00   0.00    2.00     4.00    0
.00      0.00     0.00   0.00    0.00    0.00    0.00    0.00    0.10   1.70
dm-6            16.00    896.00     0.00   0.00    3.12    56.00    0.00      0.00     0.00   0.00    0.00     0.00    0
.00      0.00     0.00   0.00    0.00    0.00    0.00    0.00    0.05   1.40
dm-7            16.00    896.00     0.00   0.00    3.00    56.00    1.00      4.00     0.00   0.00    2.00     4.00    0
.00      0.00     0.00   0.00    0.00    0.00    0.00    0.00    0.05   1.60
sda             80.00   7616.00     4.00   4.76    3.00    95.20    4.00     24.00     3.00  42.86    3.75     6.00    0
.00      0.00     0.00   0.00    0.00    0.00    3.00    3.00    0.26   2.10
sdb             24.00   2688.00     0.00   0.00    0.54   112.00    0.00      0.00     0.00   0.00    0.00     0.00    0
.00      0.00     0.00   0.00    0.00    0.00    0.00    0.00    0.01   0.50
sdc             24.00   2688.00     0.00   0.00    2.04   112.00    0.00      0.00     0.00   0.00    0.00     0.00    0
.00      0.00     0.00   0.00    0.00    0.00    0.00    0.00    0.05   1.30
zd0              4.00    448.00     0.00   0.00    0.25   112.00    0.00      0.00     0.00   0.00    0.00     0.00    0
.00      0.00     0.00   0.00    0.00    0.00    0.00    0.00    0.00   0.10
```

ภาพที่ 4-4 วัดผลกระทบของ Agent ต่อทรัพยากรระบบในสถานการณ์โหลดสูง

4.2 ผลการประเมินประสิทธิภาพด้านผู้ใช้งาน (User Metrics)

ส่วนนี้เป็นหัวใจสำคัญของการวิจัยเพื่อยืนยันว่าการบูรณาการระบบอัตโนมัติและปัญญาประดิษฐ์สามารถช่วยให้ผู้ใช้งานทั่วไปตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพจริง

4.2.1 เวลาตอบสนองของผู้ใช้ (User Response Time) คือ ระยะเวลาตั้งแต่ผู้ใช้งานได้รับข้อความแจ้งเตือนจนกระทั่งผู้ใช้งานได้ดำเนินการตอบสนองที่ถูกต้องเสร็จสิ้น โดยมีเป้าหมายความสำเร็จ (Goal) คือน้อยกว่า 90 วินาที สำหรับกรณีการโจมตีแบบ Phishing และ Bruteforce มีรายละเอียดดังตารางที่ 4-1 และ 4-2 ดังนี้

ตารางที่ 4-1 ค่ารายการสถิติเวลาตอบสนองของผู้ใช้ Phishing

รายการสถิติ Phishing	ค่าที่ได้ (วินาที)
จำนวนครั้งที่ผู้ใช้เปลี่ยนรหัส	83 ครั้ง
ค่าเฉลี่ย (Mean)	64.95
ค่าฐานนิยม (Mode)	38
ค่าน้อยที่สุด (Minimum)	15
ค่ามากที่สุด (Maximum)	120

จากตารางที่ 4-1 พบว่า จากจำนวนรายการที่มีการดำเนินการตอบสนองและเปลี่ยนรหัสผ่านสำเร็จทั้งสิ้น 83 ครั้ง มีค่าเฉลี่ย (Mean) ของเวลาที่ใช้ในการตอบสนองอยู่ที่ 64.95 วินาที อย่างไรก็ตาม เมื่อพิจารณาค่าฐานนิยม (Mode) พบว่าผู้ใช้งานกลุ่มใหญ่ที่สุดมีเวลาในการตอบสนองอยู่ที่เพียง 38 วินาที ซึ่งสะท้อนให้เห็นว่าระบบแจ้งเตือนที่พัฒนาขึ้นช่วยให้ผู้ใช้งานส่วนใหญ่ ดำเนินการได้อย่างรวดเร็ว ทั้งนี้ ข้อมูลมีขอบเขตเวลาตอบสนองสั้นที่สุด (Minimum) อยู่ที่ 15 วินาที และนานที่สุด (Maximum) อยู่ ที่ 120 วินาที (เฉพาะกรณีที่เผลอกดลิงก์ Phishing บนอีเมล Phishing จำลองเท่านั้น เนื่องจากอีก กรณีที่ไม่ได้กดลิงก์จะไม่มีระยะเวลาตอบสนองในหน่วยวินาที)

ตารางที่ 4-2 ค่ารายการสถิติเวลาตอบสนองของผู้ใช้ Bruteforce

รายการสถิติ Bruteforce	ค่าที่ได้ (วินาที)
จำนวนครั้งที่ผู้ใช้เปลี่ยนรหัส	104 ครั้ง
ค่าเฉลี่ย (Mean)	59.625
ค่าฐานนิยม (Mode)	45.6
ค่าน้อยที่สุด (Minimum)	21.3
ค่ามากที่สุด (Maximum)	119.5

จากตารางที่ 4-2 แสดงถึงค่ารายการสถิติเวลาตอบสนองของผู้ใช้ (User Response Time) สำหรับการโจมตีจำลองแบบ Bruteforce โดยพบว่าจากจำนวนการเปลี่ยนรหัสผ่านสำเร็จ 104 ครั้ง

ค่าเฉลี่ยอยู่ที่ 59.625 วินาที และมีค่าฐานนิยม (Mode) หรือระยะเวลาที่พบมากที่สุดเท่ากับ 45.6 วินาที ทั้งนี้ข้อมูลมีช่วงของการกระจายตัวตั้งแต่ค่าน้อยที่สุด (Minimum) ที่ 21.3 วินาที ไปจนถึงค่ามากที่สุด (Maximum) ที่ 119.5 วินาที ซึ่งค่าสถิติเหล่านี้สะท้อนให้เห็นว่าระบบแจ้งเตือนที่พัฒนาขึ้นช่วยให้ผู้ใช้งานส่วนใหญ่ตอบสนองต่อภัยคุกคามได้รวดเร็ว โดยมีระยะเวลาการตอบสนองส่วนมาก (Mode) อยู่ต่ำกว่าเกณฑ์มาตรฐาน 90 วินาที ที่กำหนดไว้ถึงเท่าตัว

4.2.2 อัตราการตอบสนองที่ถูกต้อง (Correct Response Rate) คือสัดส่วนของจำนวนครั้งที่ผู้ใช้งานสามารถตอบสนองต่อภัยคุกคามได้ถูกต้องตามขั้นตอนที่ได้รับการอบรม โดยมีเป้าหมายความสำเร็จ (Goal) คือ ร้อยละโดยรวมต้องมากกว่า 70%

4.2.2.1 สำหรับการจำลองสถานการณ์ภัยคุกคามไซเบอร์รูปแบบอีเมล Phishing รวมทั้งสิ้น 125 รายการ พบว่าระบบแจ้งเตือนที่พัฒนาขึ้นช่วยให้ผู้ใช้มีอัตราการตอบสนองที่ถูกต้องสูงถึงร้อยละ 70.40 (88 รายการ) โดยแบ่งออกเป็น 2 กรณีหลัก คืองานที่ไม่ได้คลิกลิงก์จำนวน 26 รายการ (ร้อยละ 20.80) และ กรณีที่ผู้ใช้งานเผลอคลิกลิงก์ แต่สามารถดำเนินการตอบสนองด้วยการเปลี่ยนรหัสผ่านได้ทันภายในเวลาที่กำหนด (ภายใน 90 วินาที) จำนวน 62 รายการ (ร้อยละ 49.60) ในส่วนของการตอบสนองที่ไม่ถูกต้อง (Incorrect Response) พบร้อยละ 29.60 (37 รายการ) ซึ่งประกอบด้วยผู้ใช้งานที่เปลี่ยนรหัสผ่านล่าช้าเกินกว่า 90 วินาทีจำนวน 21 รายการ (ร้อยละ 16.80) และผู้ใช้งานที่กดลิงก์แต่ไม่ได้ดำเนินการ เปลี่ยนรหัสผ่านตามคำแนะนำจำนวน 16 รายการ (ร้อยละ 12.80) ทั้งนี้ผลลัพธ์โดยรวมสะท้อน ให้เห็นว่าการบูรณาการระบบแจ้งเตือนร่วมกับปัญญาประดิษฐ์สามารถยกระดับความตระหนักรู้ และช่วยให้ผู้ใช้งานส่วนใหญ่ตอบสนองต่อภัยคุกคามได้อย่างถูกต้องตามเกณฑ์ที่งานวิจัยกำหนด แสดงดังตารางที่ 4-3

ตารางที่ 4-3 ค่ารายการสถิติการตอบสนองที่ถูกต้องของผู้ใช้ Phishing

รายการ	จำนวนรายก	อัตราส่วน
การตอบสนองที่ถูกต้อง	88	70.40%
ผู้ใช้ไม่ได้กดลิงก์	26	20.80%
กดลิงก์และเปลี่ยนรหัสผ่าน < 90	62	49.60%
การตอบสนองที่ไม่ถูกต้อง	37	29.60%
กดลิงก์และเปลี่ยนรหัสผ่าน > 90	21	16.80%
กดลิงก์แต่ไม่เปลี่ยนรหัสผ่าน	16	12.80%
จำนวนรายการทั้งหมด	125	100.00%

4.2.2.2 แสดงถึงค่ารายการสถิติอัตราการตอบสนองที่ถูกต้อง ของผู้ใช้ต่อการโจมตีจำลองแบบ Bruteforce โดยจากการจำลองสถานการณ์ทั้งหมด 125 รายการ พบว่าอัตราการตอบสนองที่ถูกต้องสูงถึง ร้อยละ 71.20 (89 รายการ) ซึ่งเป็น กรณีที่ผู้ใช้สามารถเปลี่ยนรหัสผ่านได้ทันภายในเวลาที่กำหนด (น้อยกว่า 90 วินาที) ในส่วนของการตอบสนองที่ไม่ถูกต้อง (Incorrect Response) มีร้อยละ 28.80 (36 รายการ) ซึ่งประกอบด้วยผู้ใช้งานที่เปลี่ยนรหัสผ่านล่าช้าเกินกว่า 90 วินาทีจำนวน 15 รายการ (ร้อยละ 12.00) และผู้ใช้งานที่ไม่ได้ดำเนินการเปลี่ยนรหัสผ่านเลย (No Respond) จำนวน 21 รายการ (ร้อยละ 16.80) ทั้งนี้ผลลัพธ์โดยรวมสะท้อนให้เห็นว่าการบูรณาการระบบแจ้งเตือนร่วมกับปัญญาประดิษฐ์สามารถช่วยให้ผู้ใช้งานส่วนใหญ่ตอบสนองต่อภัยคุกคามได้อย่างถูกต้องตามเกณฑ์ที่งานวิจัยกำหนด แสดงดังตารางที่ 4-4

ตารางที่ 4-4 ค่ารายการสถิติการตอบสนองที่ถูกต้องของผู้ใช้ Bruteforce

รายการ	จำนวนรายการ	อัตราส่วน
การตอบสนองที่ถูกต้อง	89	71.20%
เปลี่ยนรหัสผ่าน < 90 วินาที	89	71.20%
การตอบสนองที่ไม่ถูกต้อง	36	28.80%
เปลี่ยนรหัสผ่าน > 90 วินาที	15	12.00%
ไม่เปลี่ยนรหัสผ่าน	21	16.80%
จำนวนรายการทั้งหมด (นับรวมทุกกรณี)	125	100.00%

4.2.3 วิธีการวัดระดับความรู้ความเข้าใจด้านความปลอดภัย (Security Awareness Score) คือการใช้คะแนนจากแบบทดสอบ (Pre-test และ Post-test) มาเปรียบเทียบผลกัน โดยก่อนการทดลองได้มีการอบรมกลุ่มตัวอย่างเกี่ยวกับความเสี่ยงของภัยคุกคามและขั้นตอนการตอบสนองที่ถูกต้องเมื่อได้รับแจ้งเตือนจากระบบเพื่อให้ผู้ใช้งานสามารถตอบสนองต่อภัยคุกคามได้อย่างทันท่วงที ซึ่งประสิทธิภาพของการอบรมนี้ถูกวัดผลโดย Security Awareness Score โดยมีเป้าหมายความสำเร็จคือคะแนนสอบความเข้าใจหลังการทดลอง (Post-test) ต้องมากกว่า 70% จากการวิเคราะห์เปรียบเทียบคะแนนทดสอบก่อนเรียน (Pre-test) และหลังเรียน (Post-test) ของผู้ใช้จำนวน 25 ราย พบว่า คะแนนเฉลี่ยก่อนเรียนมีค่าเท่ากับ 6.88 คะแนน (S.D. = 3.49) และคะแนนเฉลี่ยหลังเรียนมีค่าเท่ากับ 16.84 คะแนน (S.D. = 2.19) ซึ่งแสดงให้เห็นว่าผู้ใช้มีความรู้

ความเข้าใจมากขึ้นอย่างชัดเจนหลังจากสิ้นสุดการวิจัย โดยคะแนนเฉลี่ยหลังเรียนเพิ่มขึ้นจากคะแนนเฉลี่ยก่อนเรียนคิดเป็นร้อยละ 144.77 สะท้อนถึงประสิทธิภาพของการอบรมและกระบวนการวิจัยที่ช่วยส่งเสริมความรู้ความเข้าใจในเนื้อหาได้อย่างมีนัยสำคัญ แสดงดังตารางที่ 4-5

ตารางที่ 4-5 ค่าสถิติความตระหนักรู้ด้านความปลอดภัยจากคะแนนแบบทดสอบ

ค่าสถิติ	Pre-test	Post-test
ค่าเฉลี่ย (Mean)	6.88	16.84
ค่ามัธยฐาน (Median)	7	16
คะแนนต่ำสุด (Min)	2	14
คะแนนสูงสุด (Max)	16	20
ส่วนเบี่ยงเบนมาตรฐาน (S.D.)	3.49	2.19

จากตารางที่ 4-5 แสดงถึงค่าสถิติความตระหนักรู้ด้านความปลอดภัยจากคะแนนแบบทดสอบ (Security Awareness Score) โดยพบว่าคะแนนเฉลี่ยหลังการทดลอง (Post-test) เพิ่มขึ้นอย่างมีนัยสำคัญจาก 6.88 คะแนน เป็น 16.84 คะแนน และมีค่าส่วนเบี่ยงเบนมาตรฐาน (S.D.) ลดลงจาก 3.49 เหลือ 2.19

เมื่อพิจารณาถึงการกระจายตัวของคะแนนพบว่าค่า มัธยฐาน (Median) เพิ่มขึ้นจาก 7 ใน Pre-test เป็น 16 คะแนนใน Post-test นอกจากนี้ ช่วงคะแนนมีการขยับขึ้นอย่างชัดเจน โดยคะแนนต่ำสุด (Min) เพิ่มจาก 2 เป็น 14 คะแนน และคะแนนสูงสุด (Max) เพิ่มจาก 16 เป็น 20 คะแนน ซึ่งผลลัพธ์เหล่านี้ยืนยันถึงประสิทธิภาพของการอบรมและกระบวนการวิจัยที่ช่วยส่งเสริมให้ผู้ใช้มีความรู้ความเข้าใจด้านความปลอดภัยมากขึ้นอย่างก้าวกระโดดและมีความสม่ำเสมอในการรับรู้ข้อมูลมากขึ้นด้วย

4.3 ผลการวิเคราะห์เชิงคุณภาพ (Qualitative Analysis)

นำเสนอผลการประเมินความเข้าใจ (จากการสอบถามความคิดเห็นแบบเปิด) และรวบรวม Feedback เชิงคำพูด (Pain Points) ที่ได้จากการทดลองใช้งานเพื่อประกอบการวิเคราะห์และปรับปรุงในขั้นตอน A: Act นี้

การวิเคราะห์เชิงคุณภาพดำเนินการโดยรวบรวมผลตอบรับเชิงคำพูด (Pain Points) ที่สำคัญจากการสอบถามความคิดเห็นแบบเปิด (Open Questions) และการสัมภาษณ์ผู้ใช้งานเพื่อระบุปัญหาที่ผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญประสบกับระบบแจ้งเตือนที่แปลผลด้วย AI เช่น ประเด็นด้าน

ความสับสนของข้อความแจ้งเตือนที่แปลผลโดย AI และความถี่ของการแจ้งเตือนที่อาจมากเกินไป ผลลัพธ์ที่ได้มีความสำคัญอย่างยิ่งต่อการวิเคราะห์และนำไปสู่การปรับปรุงระบบในขั้นตอน A: Act ตัวอย่างของ ผลตอบรับของผู้ใช้ต่อระบบมีดังนี้

- แจ้งเตือนเด้งมาบ่อยจนตกใจ บางทีก็ขัดจังหวะตอนกำลังตั้งใจทำงานอยู่ครับ
- ข้อความยาวไปนิดครับ อยากได้สรุปสั้นๆ แค่ 1-2 บรรทัดพอว่าต้องกดตรงไหน
- ปุ่มกดรับรู้บนเว็บบางทีโหลดช้าครับ นึกว่าหน้าเว็บค้างไปแล้ว
- ตอนเห็นแจ้งเตือนว่าโดนแฮกครั้งแรกตกใจมาก นึกว่าเงินในบัญชีหายไปจริงๆ แล้ว
- อยากให้มีสีบอกความรุนแรงชัดๆ เช่น สีแดงคือด่วนมาก จะได้รีบเปิดดูทันที
- สะดวกดีที่แจ้งผ่าน Telegram แต่บางทีข้อความมันดูคล้ายพวกสแปมหลอกลวงเลย
- ถ้ามีรูปภาพหรือไอคอนประกอบท่าทางการแก้ไขง่ายๆ จะดูเข้าใจง่ายกว่านี้ครับ

4.4 อภิปรายผล

งานวิจัยนี้ได้ยืนยันว่าการใช้ระบบแจ้งเตือนที่แปลผลด้วย AI และการดำเนินการปรับปรุงอย่างเป็นระบบตามวัฏจักร PDCA สามารถลดช่องว่างด้านความรู้ เพิ่มความเข้าใจในภัยคุกคามและพัฒนาประสิทธิภาพการตอบสนองต่อภัยคุกคามไซเบอร์ของผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญได้อย่างชัดเจน ดังนี้

4.4.1 การประเมินประสิทธิภาพด้านระบบของระบบบูรณาการนี้แสดงให้เห็นถึงประสิทธิภาพทางเทคนิคและความน่าเชื่อถือสูง โดยมีค่าความแม่นยำในการตรวจจับ (Detection Accuracy) อยู่ในระดับสูงสุด ด้วยค่า Precision, Recall และ F1-score เท่ากับ 1.0 (100%) ซึ่งหมายความว่าระบบสามารถดักจับและส่งแจ้งเตือนภัยคุกคามที่จำลองขึ้นได้ครบถ้วนทุกเหตุการณ์ โดยไม่มีการแจ้งเตือนที่ผิดพลาด (False Positive) หรือตรวจไม่พบ (False Negative) เลย นอกจากนี้ เวลาในการตรวจจับโดยเฉลี่ย (Average Detection Time) อยู่ที่ประมาณ 5.31 วินาที ขณะที่การใช้ทรัพยากรเครื่อง (System Performance) เช่น CPU และ Memory/RAM ของทั้ง Wazuh Server และ Agents ก็ได้รับการยืนยันว่าไม่สูงจนเกินไปและไม่ส่งผลกระทบต่อการทำงานปกติของเครื่องคอมพิวเตอร์และเครื่อง Server แม้ในสถานการณ์ที่มีโหลดสูงสุด

4.4.2 การประเมินประสิทธิภาพด้านผู้ใช้งานของการบูรณาการระบบแจ้งเตือนนี้สามารถเพิ่มประสิทธิภาพการตอบสนองได้อย่างชัดเจนในทุกด้าน สำหรับเวลาการตอบสนอง ของผู้ใช้ (User Response Time) พบว่าค่าเฉลี่ยของทั้งการโจมตีแบบ Phishing (64.95 วินาที) และ Bruteforce (59.625 วินาที) นั้น ต่ำกว่าเกณฑ์มาตรฐาน 90 วินาทีอย่างชัดเจน โดยผู้ใช้งานกลุ่มใหญ่ที่สุดมีเวลาตอบสนองรวดเร็วมาก (38 วินาที สำหรับ Phishing และ 45.6 วินาที สำหรับ Bruteforce) ในด้านอัตราการตอบสนองที่ถูกต้อง การโจมตีแบบ Phishing มีอัตรา ความถูกต้อง

สูงถึงร้อยละ 70.40 (88 รายการ) และการโจมตีแบบ Bruteforce สูงถึงร้อยละ 71.20 (89 รายการ) ซึ่งเกินกว่าเป้าหมายที่กำหนดไว้ที่ร้อยละ 70% ท้ายที่สุด ความตระหนักรู้ด้านความปลอดภัย (Security Awareness Score) ได้รับการพัฒนาอย่างมีนัยสำคัญ โดยมีคะแนนเฉลี่ยเพิ่มขึ้นจาก 6.88 เป็น 16.84 คะแนนหลังการทดลอง (เพิ่มขึ้นถึงร้อยละ 144.77) และมี ค่าส่วนเบี่ยงเบนมาตรฐาน (S.D.) ลดลงจาก 3.49 เหลือ 2.19 ซึ่งเป็นการยืนยันว่าการแจ้งเตือนที่แปลผลด้วย AI ช่วยลดช่องว่างด้านความรู้และทำให้ผู้ใช้งานมีความเข้าใจต่อภัยคุกคามได้ตามมาตรฐานเดียวกันมากขึ้น

4.5 ข้อสรุป

ผลการทดลองแสดงให้เห็นว่าระบบบูรณาการนี้มีประสิทธิภาพทางเทคนิคสูงโดยมีค่า Precision, Recall และ F1-score เท่ากับ 1.0 (100%) และเวลาในการตรวจจับเฉลี่ยอยู่ที่ประมาณ 5.31 วินาที ในด้านผู้ใช้งานพบว่า คะแนนเฉลี่ยความตระหนักรู้ด้านความปลอดภัยเพิ่มขึ้นอย่างมีนัยสำคัญจาก 6.88 เป็น 16.84 คะแนนหลังการทดลอง และค่าส่วนเบี่ยงเบนมาตรฐานลดลงอย่างชัดเจน ซึ่งยืนยันว่าการใช้ระบบแจ้งเตือนที่แปลผลด้วย AI และการดำเนินการปรับปรุงอย่างเป็นระบบตามวัฏจักร PDCA สามารถลดช่องว่างด้านความรู้ เพิ่มความเข้าใจในภัยคุกคามและพัฒนาประสิทธิภาพการตอบสนองต่อภัยคุกคามไซเบอร์ของผู้ใช้งานที่ไม่ใช่ผู้เชี่ยวชาญได้อย่างชัดเจน งานวิจัยนี้ได้สร้างแนวทางปฏิบัติที่ชัดเจนในการบูรณาการเครื่องมือ Open-Source เพื่อสร้าง เครื่องมือ Workflow Automation แบบ Real-time ที่สามารถนำไปประยุกต์ใช้ได้ในองค์กร ขนาดเล็ก

บทที่ 5
สรุปผลการวิจัย และข้อจำกัด

5.1 สรุปผลการวิจัย

งานวิจัยนี้ดำเนินการวิจัยเรื่อง การปรับปรุงประสิทธิภาพการตอบสนองต่อภัยคุกคามไซเบอร์ด้วยวัฏจักร PDCA การบูรณาการระบบตรวจจับ (Wazuh IDS) และระบบอัตโนมัติแปลผลด้วยปัญญาประดิษฐ์ (n8n/AI) โดยมีวัตถุประสงค์หลักเพื่อพัฒนาและประเมินประสิทธิภาพของระบบในการช่วยให้ผู้ใช้งานทั่วไปที่ไม่ใช่ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศว่าสามารถรับมือและตอบสนองต่อภัยคุกคามได้อย่างถูกต้องและรวดเร็วหรือไม่ ผลที่ได้รับสามารถนำไปใช้เป็นแนวทางปฏิบัติที่ชัดเจนในการบูรณาการเครื่องมือ Open-Source เพื่อสร้างเครื่องมือ Workflow Automation แบบ Real-time ที่ประยุกต์ใช้ได้ในองค์กรขนาดเล็ก ทำให้เพิ่มประสิทธิภาพในการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ได้ด้วยตนเองโดยลดการพึ่งพาผู้เชี่ยวชาญ

ผลการประเมินประสิทธิภาพด้านระบบพบว่าระบบบูรณาการมี ประสิทธิภาพทางเทคนิคสูงมากโดยมีความแม่นยำ (Precision) ความรำลึก (Recall) และ F1-score อยู่ที่ 100% (1.0) เนื่องจากสามารถดักจับและส่งแจ้งเตือนได้ครบทุกเหตุการณ์โดยไม่มีการแจ้งเตือนผิดพลาด (False Positive) หรือตรวจไม่พบ (False Negative) นอกจากนี้ยังมีเวลาในการตรวจจับเฉลี่ยเพียง 5.31 วินาที รวมถึงการใช้ทรัพยากรระบบ (CPU/RAM) ของเครื่อง Server และ เครื่องลูกข่ายยังอยู่ในเกณฑ์ที่ไม่ส่งผลกระทบต่อการทำงานปกติแม้ในสถานการณ์ที่มีโหลดสูง

ผลการทดสอบการจำลองภัยคุกคามกับกลุ่มตัวอย่างพนักงานจำนวน 25 คน จากการจำลองการโจมตีแบบ Phishing จำนวน 125 ครั้ง พบว่าผู้ใช้งานมีอัตราการตอบสนองที่ถูกต้องสูงถึง ร้อยละ 70.40 โดยมีเวลาตอบสนองเฉลี่ย 64.95 วินาที และมีค่าฐานนิยม (Mode) หรือเวลาที่พบมากที่สุดอยู่ที่เพียง 38 วินาที ในส่วนของการจำลอง การโจมตีแบบ Bruteforce จำนวน 125 ครั้ง ผู้ใช้งานมีอัตราการตอบสนองที่ถูกต้องร้อยละ 71.20 โดยมีเวลาตอบสนองเฉลี่ย 59.625 วินาที และมีค่าฐานนิยมอยู่ที่ 45.6 วินาที ซึ่งแสดงให้เห็นอย่างชัดเจนว่าระบบแจ้งเตือนที่พัฒนาขึ้นช่วยให้ผู้ใช้งานส่วนใหญ่ดำเนินการตอบสนองได้อย่างรวดเร็วต่ำกว่าเกณฑ์มาตรฐาน 90 วินาทีที่กำหนดไว้

สรุปผลด้านความตระหนักรู้ด้านความปลอดภัย (Security Awareness Score) จากการเปรียบเทียบคะแนนแบบทดสอบก่อนและหลังการทดลอง (Pre-test / Post-test) พบว่า คะแนน

เฉลี่ยเพิ่มขึ้นอย่างมีนัยสำคัญ**จาก 6.88 คะแนน เป็น 16.84 คะแนน** (เพิ่มขึ้นคิดเป็นร้อยละ 144.77) และค่าส่วนเบี่ยงเบนมาตรฐาน (S.D.) ลดลงจาก 3.49 เหลือ 2.19 ยืนยันว่าการใช้ระบบแจ้งเตือนที่แปลผลด้วย AI ร่วมกับการดำเนินงานตามวัฏจักร PDCA สามารถลดช่องว่างด้านความรู้และเพิ่มความเข้าใจในภัยคุกคามได้อย่างก้าวกระโดด

โดยสรุปแล้ว ผลจากการวิเคราะห์เชิงคุณภาพ (Qualitative Analysis) พบว่าข้อเสนอแนะจากผู้ใช้มีความสำคัญอย่างยิ่งต่อการนำไปปรับปรุงในขั้นตอน Act ซึ่งผลจากการศึกษานี้สามารถนำไปประยุกต์ใช้ในการจัดทำแผนการตอบสนองต่อเหตุการณ์ (Incident Response) แบบอัตโนมัติได้อย่างมีประสิทธิภาพและก่อให้เกิดประโยชน์อย่างแท้จริงต่อองค์กรในการเตรียมความพร้อมรับมือกับภัยคุกคามไซเบอร์ โดยการนำ AI มาทำหน้าที่เป็น "ล่าม" แปลผลข้อมูลทางเทคนิคที่ซับซ้อนให้เข้าใจง่ายได้อย่างเป็นรูปธรรม

5.2 ข้อจำกัด และข้อเสนอแนะ

เนื่องจากการศึกษานี้มุ่งเน้นกลุ่มตัวอย่างที่เป็นพนักงานทั่วไปที่ไม่ใช่ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศจำนวน 25 คน ในองค์กรขนาดเล็ก จึงอาจมีข้อจำกัดในเรื่องของขนาดและความหลากหลายของกลุ่มตัวอย่าง นอกจากนี้ การจำลองภัยคุกคามไซเบอร์ถูกออกแบบและจำกัดอยู่เพียง 2 รูปแบบหลัก คือ การส่งอีเมล Phishing จำนวน 15 รูปแบบ รวม 125 ครั้ง และการแจ้งเตือน Bruteforce จำนวน 125 ครั้ง ซึ่งอาจยังไม่ครอบคลุมภัยคุกคามทางไซเบอร์รูปแบบอื่นๆ ที่มีความซับซ้อนในสภาพแวดล้อมจริง

ในด้านระบบและเทคนิคจากการรวบรวม Feedback เชิงคำพูด (Pain Points) พบว่ามีข้อจำกัดเกี่ยวกับความล่าช้าของปุ่มกดบนระบบรายงานการถูกโจมตีที่ส่งผลต่อเวลาตอบสนองของผู้ใช้ รวมถึงรูปแบบข้อความแจ้งเตือนจาก AI ที่บางครั้งผู้ใช้งานรู้สึกตื่นตระหนก ข้อความยาวเกินไป หรือดูคล้ายข้อความสแปมหลอกลวงเสียเอง

จากข้อจำกัดดังกล่าว จึงมีข้อเสนอแนะสำหรับการปรับปรุงตามวัฏจักร PDCA ในรอบถัดไป ดังนี้

ก) ควรมีการปรับแต่ง (Fine-tune) คำสั่ง (Prompt) ของ AI อย่างต่อเนื่องเพื่อให้ข้อความแจ้งเตือนมีความกระชับ (1-2 บรรทัด) และหลีกเลี่ยงการใช้ภาษาที่ก่อให้เกิดความสับสน

ข) ควรเพิ่มการใช้องค์ประกอบทางสายตา (UI/UX) เช่น การใช้สี (สีแดงสำหรับเรื่องด่วน) หรือไอคอนประกอบท่าทางการแก้ไขเพื่อให้ผู้ใช้งานรับรู้ระดับความรุนแรงและเข้าใจได้ง่ายยิ่งขึ้น

ค) ควรประเมินและเพิ่มทรัพยากร (เช่น RAM) ให้กับระบบรายงานเพื่อแก้ไขปัญหาเวลาหน่วง (Latency) ของระบบ ซึ่งจะช่วยเพิ่มความรวดเร็วในการตอบสนองของผู้ใช้งาน

5.3 การเติมเต็มช่องว่างงานวิจัย

งานวิจัยนี้มุ่งเน้นการเติมเต็มช่องว่างที่พบในงานวิจัยก่อนหน้า ซึ่งส่วนใหญ่มักจะจำกัดอยู่เพียงมิติทางเทคนิคของระบบตรวจจับภัยคุกคาม เช่น การปรับปรุงด้านความแม่นยำของการตรวจจับและละเลยการประเมินประสิทธิภาพการตอบสนองจากมุมมองของผู้ใช้งานทั่วไป

ความแตกต่างที่สำคัญของงานวิจัยนี้คือการเปลี่ยนมามุ่งเน้นที่มุมมองของผู้ใช้งานเป็นหลัก โดยใช้ประโยชน์จากการบูรณาการระบบอัตโนมัติ (n8n) และปัญญาประดิษฐ์เพื่อทำหน้าที่แปลผลการแจ้งเตือนทางเทคนิคให้เป็นข้อความที่เข้าใจง่าย ซึ่งกลไกนี้ช่วยลดการพึ่งพาผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ในการแปลผลและแก้ไขปัญหาโดยตรง การประยุกต์ใช้ระบบ Workflow Automation และ AI ในลักษณะนี้จึงเป็นการสร้างแนวทางปฏิบัติที่เป็นรูปธรรมในการยกระดับความสามารถในการรับมือภัยคุกคามของผู้ใช้ที่ไม่ใช่ผู้เชี่ยวชาญและส่งเสริมความตระหนักรู้ด้านความปลอดภัยในองค์กรขนาดเล็กที่ขาดทรัพยากรด้านเทคโนโลยีและไซเบอร์ได้อย่างยั่งยืน

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

บรรณานุกรม

Anderson, J. P. (1980). Computer security threat monitoring and surveillance (Technical Report). James P. Anderson Company.

Chamkar, S. A., Nawari, N., & Singh, D. (2023). Improving threat detection in Wazuh using machine learning techniques. Journal of Cybersecurity and Privacy, 5(2), 34.

Deming, W. E. (1986). Out of the crisis. MIT Press.

Denning, D. E. (1987). An intrusion-detection model. IEEE Transactions on Software Engineering, 13(2), 222-232.

Gbedawo, V. W., Sedegah, K. A., & Mensah, M. A. (2017). Intrusion detection on campus network, the open-source approach: Accra Technical University case study. International Journal of Computer Applications, 164(6), 20–27.

Manzoor, J., Khalid, R., Hussain, S., & Ahmed, M. (2024). Cybersecurity on a budget: Evaluating security and performance of open source SIEM solutions for SMEs. PLOS ONE, 19(3), e0301183.

Seara, J. P., & Serrão, C. (2024). Automation of system security vulnerabilities detection using open-source software. Electronics, 13(5), 873.

ประวัติผู้เขียน

ชื่อ	นายนัทธพงศ์ วิวิธสุรการ
ชื่อการค้นคว้าอิสระ	การปรับปรุงประสิทธิภาพการตอบสนองต่อภัยคุกคามไซเบอร์ด้วยวัฏจักร PDCA: การบูรณาการระบบตรวจจับ (Wazuh IDS) และระบบอัตโนมัติแปลผลด้วยปัญญาประดิษฐ์ (n8n/AI)
สาขาวิชา	การบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
ประวัติ	ปฏิบัติงานในตำแหน่ง Senior Artificial Intelligence Engineer บริษัท บริษัท ซอฟท์เดบู จำกัด พ.ศ.2568 - ปัจจุบัน

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ