การพัฒนาเฟรมเวิร์กความปลอดภัยทางไซเบอร์ในสภาพแวดล้อมเวอร์ชวลไลเซชัน

FRAMEWORK DEVELOPMENT OF CYBERSECURITY IN A VIRTUALIZATION ENVIRONMENT

ยศวริศ คำทอง[1]* และ ทรงพล นคเรศเรืองศักดิ์[2]
Yotwarit Khamthong[1] and Songphon Nakaretruangsak [2]

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีดิจิทัลและนวัตกรรม มหาวิทยาลัยเซาธ์อีสท์บางกอก[1,2]
Master of Science Program in Information Technology, Faculty of Digital Technology and Innovation,
Southeast Bangkok University[1,2]
Author email: Yotwarit.kh@hotmail.com[1]*, Songpon@southeast.ac.th[2]

Received: September 26, 2025
Revised: December 4, 2025
Accepted: December 9, 2025

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อ 1) ออกแบบเฟรมเวิร์กความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมกับองค์กรขนาดเล็กและขนาดกลาง (SMEs) โดยผสานมาตรฐาน NIST CSF 2.0 แนวคิด Zero Trust และ Defense-in-Depth 2) พัฒนาและติดตั้งระบบต้นแบบโดยใช้เครื่องมือโอเพ่นซอร์สในสภาพแวดล้อม Proxmox VE และ 3) ประเมินประสิทธิภาพของเฟรมเวิร์กทั้งในเชิงเทคนิคและความเห็นจากผู้เชี่ยวชาญ กลุ่มตัวอย่างคือ ผู้เชี่ยวชาญจากหลายสาขาที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ จำนวน 5 ท่าน เครื่องมือที่ใช้ในการวิจัยประกอบด้วย pfSense, Wazuh, OpenVAS, Nmap, Proxmox Backup Server (PBS) และแบบประเมินความเหมาะสมของเฟรมเวิร์ก สถิติที่ใช้ในการวิเคราะห์ข้อมูล ได้แก่ ค่าเฉลี่ย (Mean) และส่วนเบี่ยงเบนมาตรฐาน (S.D.) ผลการวิจัยพบว่า 1) เฟรมเวิร์กที่พัฒนาภายใต้กรอบ Design Science Research (DSR) ประกอบด้วยองค์ประกอบหลักตามหน้าที่ของ NIST CSF 2.0 ทั้ง 6 หน้าที่ (Govern, Identify, Protect, Detect, Respond, Recover) สามารถบูรณาการเครื่องมือโอเพ่นซอร์สทั้ง 5 รายการเข้ากับกระบวนการทำงานได้อย่างสมบูรณ์ 2) ผลการประเมินความเหมาะสมของเฟรมเวิร์กโดยผู้เชี่ยวชาญพบว่า มีความเหมาะสมในระดับมากถึงมากที่สุด (ค่าเฉลี่ย 4.76 จาก 5.00) ครอบคลุมทั้ง 6 หน้าที่หลักของ NIST CSF 2.0 โดยนโยบายและ SOPs ได้คะแนนสูงสุด (4.84) รองลงมาคือแบบฟอร์ม (4.80) และ Runbooks (4.64) และการทดสอบระบบต้นแบบยืนยันประสิทธิภาพในทางปฏิบัติ สามารถลดจำนวนช่องโหว่ได้อย่างมีนัยสำคัญ ตรวจจับและตอบสนองต่อภัยคุกคามได้ทันท่วงที และบรรลุเป้าหมาย RTO ตามที่กำหนด และ 3) การทดสอบระบบต้นแบบพบว่าการทดสอบด้านการบริหารจัดการความเสี่ยงสามารถลดจำนวนช่องโหว่ได้อย่างมีนัยสำคัญ ตรวจจับและตอบสนองต่อภัยคุกคามได้ทันท่วงที และบรรลุเป้าหมายระยะเวลาในการการกู้คืน (RTO) หลังการโจมตีได้ตามที่กำหนดซึ่งสะท้อนให้เห็นถึงความมีประสิทธิภาพและศักยภาพในการประยุกต์ใช้งานจริงสำหรับ SMEs และสามารถต่อยอดพัฒนาสู่ระบบตอบสนองอัตโนมัติในอนาคต

คำสำคัญ: NIST Cybersecurity Framework, Proxmox VE, ความปลอดภัยทางไซเบอร์, โอเพ่นซอร์ส, เวอร์ชวลไลเซชัน

Abstract

This research aimed to: 1) design a cybersecurity framework suitable for small and medium-sized enterprises (SMEs) by integrating the NIST Cybersecurity Framework (CSF) 2.0, Zero Trust principles, and the Defense-in-Depth concept; 2) develop and deploy a prototype system using open-source tools within a Proxmox VE environment; and 3) evaluate the effectiveness of the proposed framework in terms of technical performance and expert judgment.The sample group consisted of five experts from multidisciplinary fields related to cybersecurity. The research instruments included pfSense, Wazuh, OpenVAS, Nmap, Proxmox Backup Server (PBS), and a framework suitability assessment form. Data were analyzed using mean and standard deviation.

The results indicated that: 1) the framework developed under the Design Science Research (DSR) approach comprised core components aligned with all six functions of NIST CSF 2.0—Govern, Identify, Protect, Detect, Respond, and Recover—and successfully integrated all five open-source tools into the operational workflow; 2) expert evaluation demonstrated that the framework achieved a high to very high level of appropriateness, with an overall mean score of 4.76 out of 5.00, covering all six core functions of NIST CSF 2.0, where policies and standard operating procedures (SOPs) received the highest score (4.84), followed by operational forms (4.80) and runbooks (4.64); and 3) prototype system testing confirmed practical effectiveness, showing a significant reduction in system vulnerabilities, timely threat detection and response, and successful achievement of the defined Recovery Time Objective (RTO). These results reflect the effectiveness and applicability of the proposed framework for SMEs and indicate its potential for further development toward automated cybersecurity response systems in the future.

Keywords: NIST Cybersecurity Framework, Proxmox VE, Cybersecurity, Open-Source, Virtualization

บทนำ

การเปลี่ยนผ่านสู่ระบบดิจิทัล (Digital Transformation) ได้สร้างการเปลี่ยนแปลงครั้งใหญ่ต่อกระบวนการดำเนินงานขององค์กรในทุกภาคส่วน ส่งผลให้ขอบเขตของระบบสารสนเทศขยายตัวอย่างรวดเร็ว และก่อให้เกิดพื้นที่การโจมตี (Attack Surface) ที่กว้างขึ้นอย่างมีนัยสำคัญ สถานการณ์ภัยคุกคามไซเบอร์ในปัจจุบันมีความซับซ้อนและรุนแรงยิ่งขึ้น โดยเฉพาะการใช้บัญชีที่ถูกขโมย (Valid Accounts) ซึ่งกลายเป็นช่องทางการโจมตีที่พบบ่อยที่สุดคิดเป็น 30% ของเหตุการณ์ทั้งหมด ตามรายงาน IBM X-Force Threat Intelligence Index 2024 [1] ขณะที่เป้าหมายหลักของการโจมตียังคงเป็นโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure) ซึ่งสร้างความเสียหายต่อความต่อเนื่องทางธุรกิจ (Business Continuity) โดยตรง [2], [3], [4]

ในบริบทนี้ เทคโนโลยีเวอร์ชวลไลเซชัน (Virtualization) ซึ่งเป็นแกนกลางของการบริหารจัดการระบบสารสนเทศสมัยใหม่ กลับกลายเป็นจุดอ่อนสำคัญที่ผู้ประสงค์ร้ายให้ความสนใจ โดยเฉพาะ Hypervisor ที่ทำหน้าที่ควบคุมและบริหารจัดการเครื่องเสมือนทั้งหมด [5], [6] หากถูกโจมตีสำเร็จ จะสามารถเข้าควบคุมโครงสร้างพื้นฐานทั้งระบบได้ทันที เหตุการณ์

การโจมตีด้วยแรนซัมแวร์ที่มุ่งเป้าไปยังช่องโหว่ของ VMware ESXi ได้ตอกย้ำถึงความเปราะบางของระบบดังกล่าว [7] และข้อมูลจาก ENISA Threat Landscape 2024 ยังยืนยันว่าแรนซัมแวร์ยังคงเป็นภัยคุกคามอันดับหนึ่ง พร้อมแนวโน้มการโจมตีระบบเวอร์ชวลไลเซชันที่เพิ่มสูงขึ้นต่อเนื่อง [8]

แม้องค์กรจะมีการปรับตัวโดยพัฒนาแนวทางการป้องกันภัยไซเบอร์อย่างต่อเนื่อง แต่จากการทบทวนวรรณกรรมพบว่า โซลูชันที่มีอยู่ส่วนใหญ่มักพึ่งพาระบบเชิงพาณิชย์ขนาดใหญ่ เช่น VMware หรือ AWS และขาดการประยุกต์ใช้ที่เหมาะสมกับองค์กรที่มีข้อจำกัดด้านทรัพยากร โดยเฉพาะองค์กรขนาดกลางและขนาดย่อม (SMEs) [9], [10] ที่นิยมใช้ระบบโอเพ่นซอร์สอย่าง Proxmox Virtual Environment (Proxmox VE) [11], [12], [13] ซึ่งยังขาดแนวทางที่ชัดเจนในการบูรณาการกับมาตรฐานความมั่นคงปลอดภัยระดับสากล [14], [15]

จากการทบทวนงานวิจัยที่เกี่ยวข้อง พบว่ามีงานวิจัยของ Grad [16] ได้นำเสนอแนวทางการประยุกต์ใช้ NIST CSF 2.0 [17], [18], [19] ร่วมกับโมเดล Zero Trust [20] สำหรับองค์กรไม่แสวงหากำไร ซึ่งมีแนวคิดที่สอดคล้องกับงานวิจัยนี้ อย่างไรก็ตามงานวิจัยดังกล่าวยังเน้นที่กรอบแนวคิดและการวางแผนเชิงนโยบายเป็นหลัก และยังขาดการนำเสนอรายละเอียดเชิงเทคนิคในการติดตั้งใช้งานจริง (Technical Implementation) ในสภาพแวดล้อมเวอร์ชวลไลเซชัน แบบโอเพ่นซอร์ส [21], [22], [23], [24], [25] ดังนั้น งานวิจัยฉบับนี้จึงมุ่งเน้นที่จะเติมเต็มช่องว่างดังกล่าว (Research Gap) โดยนำเสนอคุณูปการของงานวิจัย (Contribution) ผ่านการพัฒนาเฟรมเวิร์กความมั่นคงปลอดภัยแบบ End-to-End ที่บูรณาการทั้ง NIST CSF 2.0, Zero Trust และ Defense-in-Depth เข้าด้วยกัน และสามารถนำไปติดตั้งใช้งานได้จริงบนแพลตฟอร์ม Proxmox VE โดยใช้เครื่องมือโอเพ่นซอร์สแบบครบวงจร [26], [27], [28], [29], [30], [31], [32] ดังนั้น งานวิจัยฉบับนี้จึงมีเป้าหมายในการพัฒนากรอบการดำเนินงานต้นแบบ (Prototype Framework) [33] ที่สามารถสร้างระบบที่ปลอดภัยและสามารถตรวจจับ-ตอบสนอง-ฟื้นตัวได้อย่างทันท่วงที โดยออกแบบให้เหมาะสมกับข้อจำกัดของ SMEs และสามารถตอบสนองต่อภัยคุกคามที่มุ่งเป้าระบบเวอร์ชวลไลเซชัน ได้อย่างมีประสิทธิภาพ

วัตถุประสงค์การวิจัย

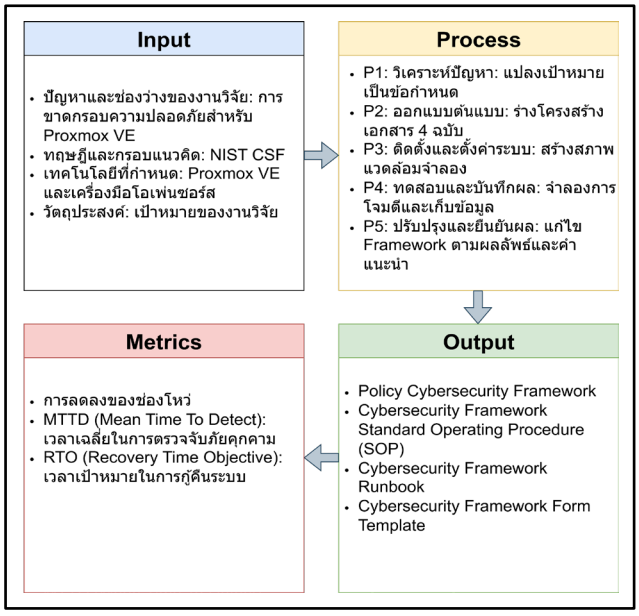
1. เพื่อออกแบบเฟรมเวิร์กความมั่นคงปลอดภัยไซเบอร์โดยผสาน NIST CSF กับ Proxmox VE และเครื่องมือโอเพ่นซอร์ส
2. เพื่อพัฒนาและติดตั้งระบบต้นแบบโดยใช้เครื่องมือโอเพ่นซอร์สในสภาพแวดล้อม Proxmox VE
3. เพื่อประเมินประสิทธิภาพของเฟรมเวิร์กทั้งในเชิงเทคนิคและความเห็นจากผู้เชี่ยวชาญ

วิธีดำเนินการวิจัย

ขั้นตอนการดำเนินการวิจัย วิธีการเก็บข้อมูลในการวิจัย ให้ระบุขั้นตอน หรือระยะที่ดำเนินการวิจัยเป็นข้อ ๆ ตามลำดับการวิจัย ระบุเครื่องมือที่ใช้ และการหาคุณภาพของเครื่องมือที่นำใช้ในการทำวิจัย

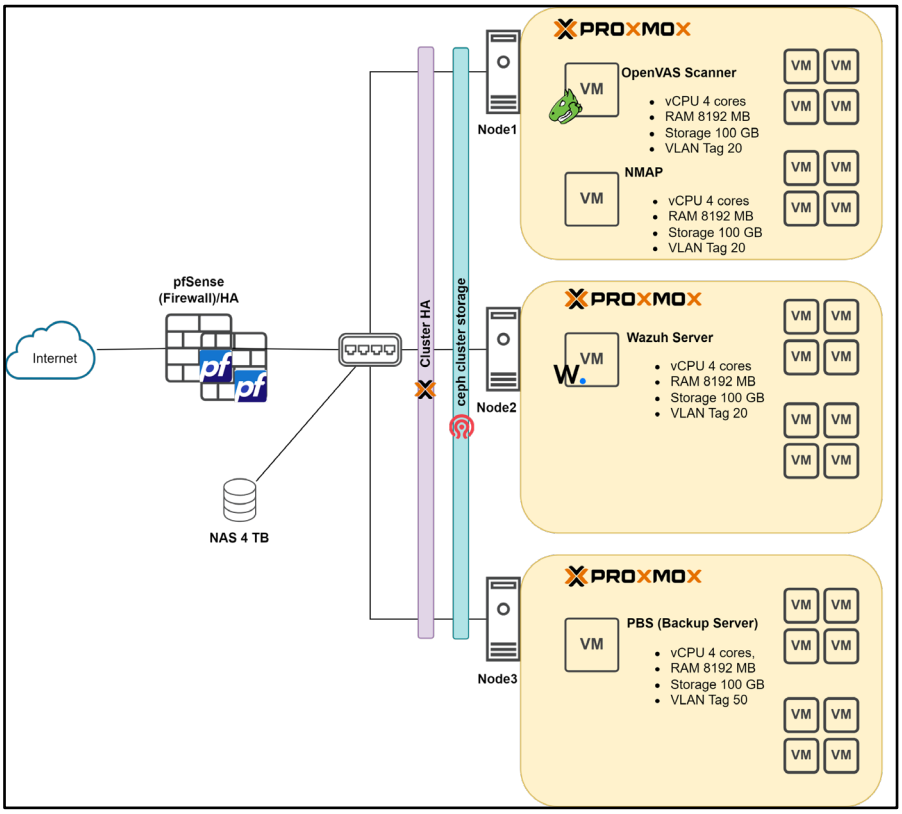
1. ขั้นตอนการดำเนินการวิจัย

1.1 การวิจัยนี้ดำเนินการตามกรอบ Design Science Research (DSR) โดยมีรายละเอียดในแต่ละขั้นตอนดังแสดงในรูปที่ 1 ซึ่งประกอบด้วยกระบวนการ 5 ระยะ (P1-P5) ได้แก่ P1-การวิเคราะห์ปัญหาเพื่อกำหนดขอบเขต, P2-การออกแบบโครงสร้างเฟรมเวิร์กเอกสาร, P3-การติดตั้งระบบทดสอบบน Proxmox VE, P4-การทดสอบจำลองสถานการณ์ภัยคุกคาม และ P5-การปรับปรุงผลลัพธ์สำหรับตัวชี้วัด (Metrics) ที่ใช้ประเมินประสิทธิภาพ ได้แก่ อัตราการลดลงของช่องโหว่, ค่าเฉลี่ยเวลาในการตรวจจับ (MTTD) และระยะเวลาเป้าหมายในการกู้คืนระบบ (RTO) แสดงดังรูปที่ 1



รูปที่ 1 กระบวนการพัฒนา Framework

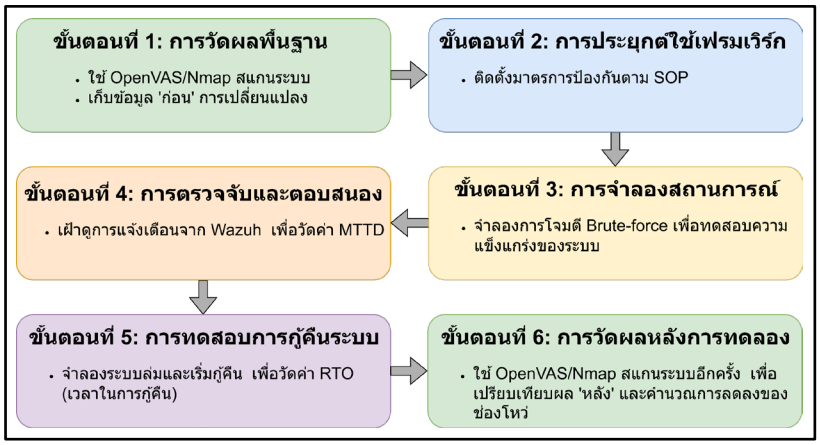
1.2 การประยุกต์ใช้ในบริบทจริง (Implementation): ติดตั้งเฟรมเวิร์กต้นแบบในระบบเสมือน (Virtual Lab) ที่จำลองสภาพแวดล้อมขององค์กร SMEs การติดตั้งระบบในบริบทจริงใช้ Proxmox VE เป็นแกนหลัก โดยแบ่งส่วนเครือข่ายด้วยVLAN เครื่องมือ pfSense ทำหน้าที่ Firewall Wazuh ทำหน้าที่ SIEM ตรวจจับภัยคุกคาม OpenVAS NMAP Vulnerability Scaner และ Proxmox Backup Server (PBS) ใช้สำหรับการกู้คืนข้อมูล แสดงดังรูปที่ 2



รูปที่ 2 การประยุกต์ใช้ในบริบทจริง

1.3 การประเมินผลเชิงประจักษ์ (Evaluation): กระบวนการประเมินผลเชิงประจักษ์ เริ่มต้นด้วยการวัดผลพื้นฐาน เพื่อจัดเก็บข้อมูลสถานะความปลอดภัยก่อนการเปลี่ยนแปลง โดยใช้เครื่องมือ OpenVAS และ Nmap สแกนระบบเพื่อบันทึกจำนวนช่องโหว่ตามระดับความเสี่ยง (CVE) และสถานะของพอร์ตที่เปิดใช้งานเพื่อใช้เป็นเกณฑ์เปรียบเทียบ จากนั้นจึงดำเนินการ ประยุกต์ใช้เฟรมเวิร์ก โดยติดตั้งมาตรการป้องกันตามมาตรฐานปฏิบัติงาน (SOP) ที่กำหนดไว้ เมื่อระบบมีความพร้อมจะเข้าสู่การจำลองสถานการณ์ ซึ่งงานวิจัยนี้เลือกใช้การโจมตีแบบ Brute-force เป็นกรณีทดสอบหลัก เนื่องจากเป็นภัยคุกคามพื้นฐานที่พบบ่อยและสามารถชี้วัดประสิทธิภาพของนโยบายรหัสผ่านและระบบป้องกันการบุกรุกได้อย่างชัดเจน ควบคู่ไปกับการตรวจจับและตอบสนองผ่านระบบ Wazuh เพื่อวัดค่าระยะเวลาเฉลี่ยในการตรวจจับ (MTTD)

ในส่วนของการทดสอบความต่อเนื่องทางธุรกิจ ผู้วิจัยได้ดำเนินการทดสอบการกู้คืนระบบ โดยจำลองสถานการณ์วิกฤตผ่านการหยุดการทำงานของบริการหลัก เพื่อให้ระบบไม่สามารถให้บริการได้แล้วดำเนินการกู้คืนสถานะด้วยกระบวนการย้อนค่า (Backup Restore) เพื่อจับเวลาและคำนวณค่า Recovery Time Objective (RTO) และสิ้นสุดกระบวนการด้วย การวัดผลหลังการทดลอง โดยการสแกนระบบซ้ำภายใต้สภาพแวดล้อมเดิม เพื่อนำผลลัพธ์มาวิเคราะห์เปรียบเทียบพัฒนาการของการลดช่องโหว่และการรักษาความปลอดภัยที่เพิ่มขึ้นหลังการปรับปรุงระบบ แสดงดังรูปที่ 3



รูปที่ 3 การประเมินผลเชิงประจักษ์

2. เครื่องมือวิจัยและการติดตั้งระบบ

ในการดำเนินงานวิจัย มีการจัดเตรียมโครงสร้างพื้นฐานสำหรับทดสอบดังนี้

2.1 Proxmox VE: เป็นแพลตฟอร์มเวอร์ชวลไลเซชันหลักของระบบต้นแบบ

2.2 Open-source Security Tools: เช่น Wazuh (SIEM), OpenVAS และ Nmap (Vulnerability Scanner), Proxmox Backup Server (PBS) สำหรับการตรวจจับแจ้งเตือน และกู้คืนข้อมูล

2.3 NIST CSF Mapping Template: สำหรับการจัดกลุ่มและกำหนด Policy ตามฟังก์ชันของ CSF (Identify, Protect, Detect, Respond, Recover, Govern) มีการออกแบบแผนผังเครือข่ายทดสอบในลักษณะ Defense-in-Depth พร้อมแบ่งสิทธิการเข้าถึงตามแนวทาง Zero Trust และกำหนดระยะเวลาในการจำลองเหตุการณ์ภัยคุกคาม

3. ประชากรและกลุ่มตัวอย่าง

3.1 ประชากร: ได้แก่ ผู้เชี่ยวชาญที่มีความรู้และประสบการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ เทคโนโลยีสารสนเทศ และระบบเครือข่าย

3.2 กลุ่มตัวอย่าง: วิธีการเลือกแบบเจาะจง จำนวน 5 ท่าน โดยมีเกณฑ์การคัดเลือกคือต้องเป็นผู้ที่มีประสบการณ์ทำงานในสายงานที่เกี่ยวข้องไม่น้อยกว่า 3 ปี เพื่อให้มั่นใจว่าผู้ประเมินมีความเชี่ยวชาญเพียงพอในการตรวจสอบความเหมาะสมของเฟรมเวิร์ก

4. วิธีการเก็บข้อมูล

4.1 การประเมินช่องโหว่: ใช้ OpenVAS สแกนก่อนและหลังติดตั้งเฟรมเวิร์ก เพื่อเปรียบเทียบระดับความรุนแรง (Severity) และจำนวนช่องโหว่

4.2 การจำลองภัยคุกคาม: ทดสอบโดยใช้เทคนิคจำลองพฤติกรรมของผู้โจมตี Brute-force

4.3 การบันทึกเวลาในการกู้คืน: ใช้ค่า Recovery Time Objective (RTO) เป็นเกณฑ์ในการวัดความสามารถของระบบหลังเกิดเหตุ

5. การวิเคราะห์ข้อมูล

5.1 วิเคราะห์เชิงเปรียบเทียบก่อนและหลังติดตั้งเฟรมเวิร์ก

5.2 วัดค่าประสิทธิภาพตามตัวชี้วัด 3 ด้านหลัก ได้แก่

5.2.1 จำนวนช่องโหว่ลดลง (Vulnerability Reduction)

5.2.2 ความสามารถในการตรวจจับ (Detection Accuracy)

5.2.3 เวลากู้คืนระบบ (RTO Compliance)

ผลการวิจัย

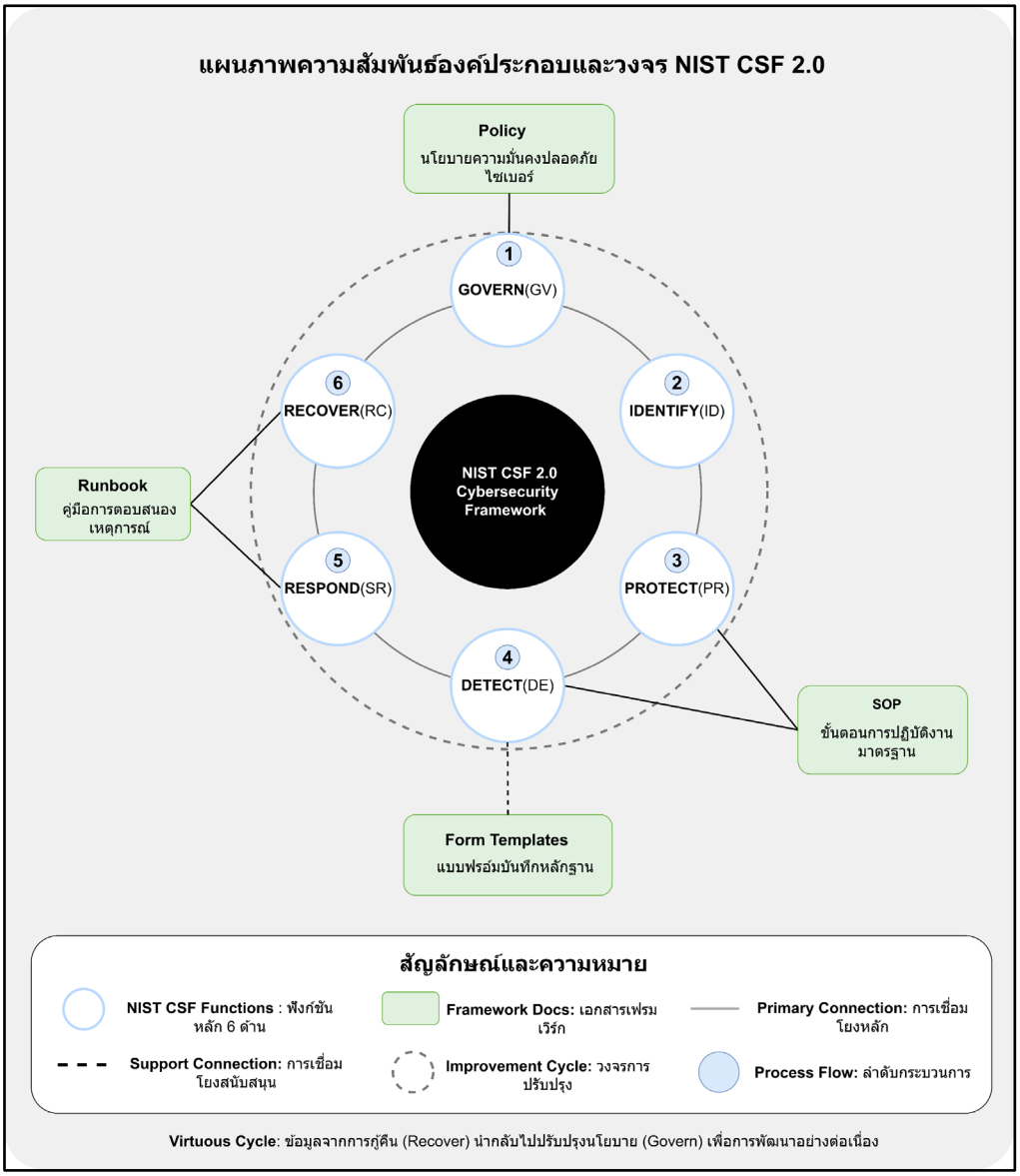
1. ผลการออกแบบและพัฒนาเฟรมเวิร์กต้นแบบ

ผลผลิตสำคัญของการวิจัยครั้งนี้ คือ ชุดเอกสาร Prototype Cybersecurity Framework จำนวน 4 ฉบับ ซึ่งได้รับการออกแบบให้เชื่อมโยงอย่างเป็นระบบกับวงจรการบริหารจัดการตามแนวทาง NIST Cybersecurity Framework (CSF) เวอร์ชัน 2.0 โดยแต่ละเอกสารถูกจัดกลุ่มตามฟังก์ชันหลัก ได้แก่ Govern, Identify, Protect, Detect, Respond และ Recover พร้อมทั้งประยุกต์ร่วมกับแนวคิด Zero Trust และ Defense-in-Depth ผ่านการแบ่งส่วนเครือข่ายและการจำกัดสิทธิ์การเข้าถึงให้น้อยที่สุด ควบคู่กับการบูรณาการเครื่องมือโอเพ่นซอร์สในระบบ Proxmox VE

เอกสารประกอบเฟรมเวิร์กที่พัฒนาขึ้น ประกอบด้วย

1) เอกสารนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ (Policy)
2) เอกสารกระบวนการปฏิบัติงานมาตรฐาน (Standard Operating Procedures - SOPs)
3) คู่มือปฏิบัติการตอบสนองเหตุการณ์ (Runbooks)
4) ชุดแบบฟอร์มและเทมเพลต (Form Templates)

ทั้งนี้ เอกสารแต่ละชุดมีความสอดคล้องกับมาตรฐานสากล เช่น NIST CSF, ISO/IEC 27001, และแนวทาง Zero Trust โดยมีเป้าหมายเพื่อให้สามารถนำไปใช้งานในสภาพแวดล้อมจริงขององค์กรขนาดกลางและขนาดเล็ก (SMEs) ได้อย่างเป็นรูปธรรม



รูปที่ 4 ความสัมพันธ์ขององค์ประกอบเฟรมเวิร์กกับวงจร NIST CSF

จากรูปที่ 4 แสดงกรอบการทำงานที่บูรณาการร่วมกับวงจร NIST CSF 2.0 โดยหัวใจสำคัญที่ทำให้เฟรมเวิร์กนี้เกิดประสิทธิภาพสูงสุดคือ Virtuous Cycle หรือกลไกการเรียนรู้และพัฒนาอย่างต่อเนื่อง ซึ่งปรากฏในแผนภาพในรูปแบบของวงจรการปรับปรุง (Improvement Cycle) ที่เป็นเส้นประเชื่อมโยงกระบวนการทั้งหมดเข้าด้วยกัน

กระบวนการทำงานของ Virtuous Cycle ทำหน้าที่เป็นกลไกการป้อนกลับข้อมูล (Feedback Loop) กล่าวคือ เมื่อองค์กรเสร็จสิ้นขั้นตอน การกู้คืนระบบ (Recover) ข้อมูลเหตุการณ์และบทเรียนที่ได้รับ (Lessons Learned) จะถูกนำกลับไปวิเคราะห์เพื่อปรับปรุงนโยบาย (Policy) ในฟังก์ชันการกำกับดูแล (Govern) ให้มีความรัดกุมและทันสมัยยิ่งขึ้น ดังคำอธิบายที่ระบุไว้ส่วนล่างของแผนภาพ ส่งผลให้มาตรการป้องกัน (Protect) และการตรวจจับ (Detect) ในรอบถัดไปมีประสิทธิภาพสูงขึ้นเกิดเป็นการยกระดับความปลอดภัยที่ไม่สิ้นสุด

เพื่อให้เห็นภาพการนำเฟรมเวิร์กไปปฏิบัติจริงได้ชัดเจนยิ่งขึ้น ผู้วิจัยขอยกตัวอย่างรายละเอียดของเอกสารในองค์ประกอบหลัก ได้แก่ ขั้นตอนการปฏิบัติงานมาตรฐาน (SOPs) สำหรับการจัดการช่องโหว่ดังแสดงในรูปที่ 5 และคู่มือการตอบสนองเหตุการณ์ (Runbook) สำหรับ Brute-force ดังแสดงในรูปที่ 6

9. IDENTIFY-PROC-Vulnerability-Assessment

วัตถุประสงค์: เพื่อกำหนดขั้นตอนในวงจรการบริหารจัดการช่องโหว่ (Vulnerability Management Lifecycle) ตั้งแต่การค้นหา, การรายงาน, การติดตามการแก้ไข, และการทวนสอบผลอย่างเป็นระบบ

ขอบเขต:

- **การประเมินช่องโหว่ (Vulnerability Assessment - VA):** ครอบคลุมทรัพย์สินสารสนเทศทั้งหมดที่ระบุไว้ใน CMDB
- **การทดสอบเจาะระบบ (Penetration Testing - PT):** ครอบคลุมระบบงานที่มีระดับความสำคัญ Tier 0 และ Tier 1 หรือระบบที่เปิดให้เข้าถึงได้จากเครือข่ายอินเทอร์เน็ต

ขั้นตอนการปฏิบัติ:

1. **การประเมินช่องโหว่ (Vulnerability Assessment - VA):**
   - **การสแกนตามกำหนดเวลา:** การสแกนเครือข่ายภายในทั้งหมดโดยอัตโนมัติเป็นรายสัปดาห์ (ในช่วงนอกเวลาทำการ) จะต้องถูกดำเนินการโดย OpenVAS
   - **การแจ้งเตือน:** เมื่อการสแกนเสร็จสิ้น, ผลลัพธ์จะต้องถูกส่งต่อไปยัง Wazuh ซึ่งจะทำการวิเคราะห์และสร้างการแจ้งเตือน (Alert) สำหรับช่องโหว่ที่มีคะแนน CVSS ตั้งแต่ 7.0 ขึ้นไป
   - **การสร้าง Ticket:** Ticket สำหรับช่องโหว่แต่ละรายการจะต้องถูกสร้างขึ้นในระบบติดตามงานโดยทีมความมั่นคงปลอดภัยไซเบอร์ และมอบหมายให้เจ้าของระบบ (System Owner) ดำเนินการแก้ไข
   - **ข้อตกลงระดับการให้บริการ (SLA) ในการแก้ไข:**
     - **Critical (CVSS 9.0-10.0):** ภายใน 7 วันทำการ
     - **High (CVSS 7.0-8.9):** ภายใน 30 วันทำการ
     - **Medium (CVSS 4.0-6.9):** ภายใน 90 วันทำการ
   - **การสแกนซ้ำเพื่อทวนสอบ (Verification Scan):** หลังจากที่เจ้าของระบบแจ้งปิด Ticket, การสแกนซ้ำที่เป้าหมายเดิมเพื่อทวนสอบว่าช่องโหว่ได้รับการแก้ไขอย่างสมบูรณ์จะต้องถูกดำเนินการโดย OpenVAS ก่อนที่จะทำการปิด Ticket อย่างเป็นทางการ

รูปที่ 5 ตัวอย่างขั้นตอนการปฏิบัติงานมาตรฐาน (SOP) สำหรับการจัดการช่องโหว่

17. DETECT-RUNBOOK-Threat-Triage-v1.0

เอกสารนโยบายที่เกี่ยวข้อง: DETECT-PROC-Threat-Monitoring-v1.0

วัตถุประสงค์: เพื่อวิเคราะห์และคัดกรองการแจ้งเตือน (Alert) ที่เกิดขึ้นใน Wazuh Dashboard อย่างเป็นระบบ, ตัดสินใจ, และยกระดับเป็นเหตุการณ์ละเมิด (Incident) หากมีความจำเป็น

ผู้รับผิดชอบ: นักวิเคราะห์ความมั่นคงปลอดภัย (L1)

เงื่อนไขการริเริ่มกระบวนการ: การเฝ้าระวังอย่างต่อเนื่องตลอดเวลาทำการ (Continuous Monitoring)

ขั้นตอนการปฏิบัติ:

1. **การเฝ้าระวัง Dashboard:** ใช้หน้าจอ "Security Events" ใน Wazuh เป็นเครื่องมือหลักในการเฝ้าระวังแบบ Real-time
2. **การจัดลำดับความสำคัญ:** ให้ความสำคัญกับการแจ้งเตือนที่มีระดับความรุนแรง (Rule Level) ตั้งแต่ 10-15 เป็นอันดับแรก เนื่องจากมีความเป็นไปได้สูงที่จะเป็นภัยคุกคามที่เกิดขึ้นจริง
3. **การวิเคราะห์การแจ้งเตือน:**
    - คลิกที่การแจ้งเตือนเพื่อดูรายละเอียดทั้งหมด: Rule Description, MITRE ATT&CK Tactic/Technique, Source IP, Destination IP, User, File path, Process name
    - ตรวจสอบข้อมูลแวดล้อม (Contextual Information) เช่น บันทึกเหตุการณ์ก่อนและหลังเวลาที่เกิด, ประวัติการแจ้งเตือนที่เคยเกิดบน Host เดียวกัน, ข้อมูล Threat Intelligence ของ IP Address ที่เกี่ยวข้อง
    - พิจารณาและจำแนกว่าเป็น True Positive (เหตุการณ์จริง) หรือ False Positive (การแจ้งเตือนที่ผิดพลาด)
        - **ตัวอย่าง True Positive:** ความพยายามในการทำ Brute-force SSH จาก IP ที่ไม่รู้จัก, การรันคำสั่ง PowerShell ที่น่าสงสัย, การตรวจพบ Signature ของมัลแวร์
        - **ตัวอย่าง False Positive:** การเข้าสู่ระบบที่ล้มเหลวหลายครั้งโดยผู้ใช้ที่ทราบว่าลืมรหัสผ่าน, การแจ้งเตือนที่เกิดจากการสแกนช่องโหว่ตามกำหนดการ

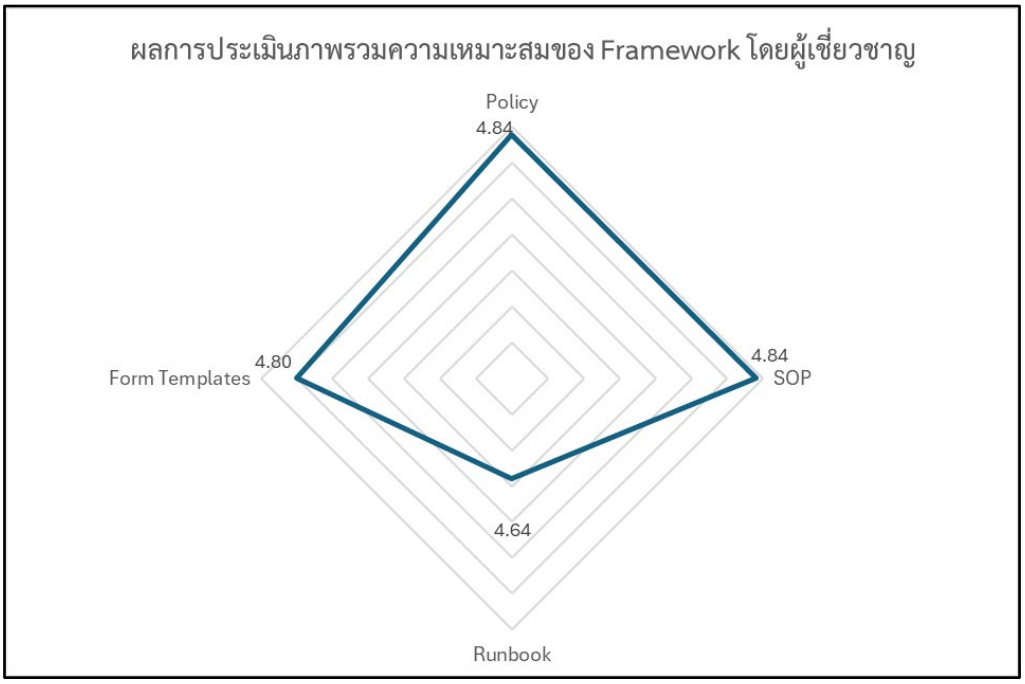
รูปที่ 6 ตัวอย่างคู่มือการตอบสนองเหตุการณ์ (Runbook) กรณี Brute-force

ภายหลังการพัฒนาเฟรมเวิร์กและเอกสารประกอบสำหรับใช้งานบนระบบ Proxmox VE ผู้วิจัยได้จัดกระบวนการประเมินความเหมาะสมและความน่าเชื่อถือโดยผู้เชี่ยวชาญโดยมีเกณฑ์การคัดเลือกคือ ต้องเป็นผู้ที่มีประสบการณ์ทำงานในสายงานที่เกี่ยวข้องไม่น้อยกว่า 3 ปี จำนวน 5 ท่าน ด้วยเทคนิคเดลฟาย (Delphi Technique) จำนวน 2 รอบ ซึ่งรอบแรกเป็นการรวบรวมข้อเสนอแนะเพื่อการปรับปรุง และรอบที่สองเป็นการประเมินเฟรมเวิร์กฉบับแก้ไขสมบูรณ์แล้ว โดยมีผลการประเมินความเหมาะสมในแต่ละด้านดังแสดงในตารางที่ 1

ตารางที่ 1 ผลการประเมินภาพรวมความเหมาะสมของ Framework โดยผู้เชี่ยวชาญ

องค์ประกอบของ Framework	$\bar{x}$	S.D.
1. ด้านนโยบาย (Policy)	4.84	0.26
2. ด้านกระบวนการ (SOP)	4.84	0.26
3. ด้านคู่มือตอบสนอง (Runbook)	4.64	0.26
4. ด้านชุดแบบฟอร์ม (Form Templates)	4.80	0.24
ผลรวมค่าเฉลี่ย	**4.78**	**0.05**

จากผลการประเมินโดยผู้เชี่ยวชาญทั้ง 5 ท่านในรอบที่ 2 พบว่า เฟรมเวิร์กต้นแบบมีความเหมาะสมในระดับ มากถึงมากที่สุด ครอบคลุม 4 องค์ประกอบหลัก ได้แก่ นโยบาย (Policy), ขั้นตอนปฏิบัติงาน (SOPs), คู่มือการรับมือเหตุการณ์ (Runbooks) และแบบฟอร์ม (Form Templates) แสดงดังรูปที่ 7



รูปที่ 7 ผลการประเมินภาพรวมความเหมาะสมของ Framework โดยผู้เชี่ยวชาญ

จากรูปที่ 7 ผลการประเมินภาพรวมความเหมาะสมของ Framework โดยผู้เชี่ยวชาญโดยมีรายละเอียดที่โดดเด่นดังนี้

1) ด้านนโยบาย ได้คะแนนเฉลี่ย 4.84 (SD = 0.26) แสดงถึงความชัดเจนครอบคลุม และสอดคล้องกับมาตรฐาน NIST CSF และ Zero Trust ช่วยกำหนดกรอบการดำเนินงานด้านความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ

2) ด้าน SOPs มีคะแนนเฉลี่ยเท่ากันที่ 4.84 (SD = 0.26) สะท้อนถึงความเป็นระบบ เข้าใจง่าย และสามารถนำไปใช้ปฏิบัติจริงได้อย่างสม่ำเสมอ

3) ด้าน Runbooks ได้คะแนนเฉลี่ย 4.64 (SD = 0.26) โดยเฉพาะความสามารถในการลดเวลาในการตอบสนอง (MTTR) และการกู้คืนระบบ (RTO) แสดงถึงศักยภาพในการรองรับเหตุการณ์ฉุกเฉิน

4) ด้านแบบฟอร์ม ได้คะแนนเฉลี่ย 4.80 (SD = 0.24) เด่นชัดในด้านความชัดเจนประโยชน์ใช้สอย และการสนับสนุนระบบการจัดเก็บข้อมูลและตรวจสอบย้อนหลัง (Audit Trail)

โดยสรุปเฟรมเวิร์กที่พัฒนาขึ้นมีความสมดุลทั้งในเชิงนโยบายแนวปฏิบัติ และเครื่องมือสนับสนุนสามารถนำไปประยุกต์ใช้ในองค์กรได้อย่างเป็นระบบและสอดคล้องกับมาตรฐานสากล

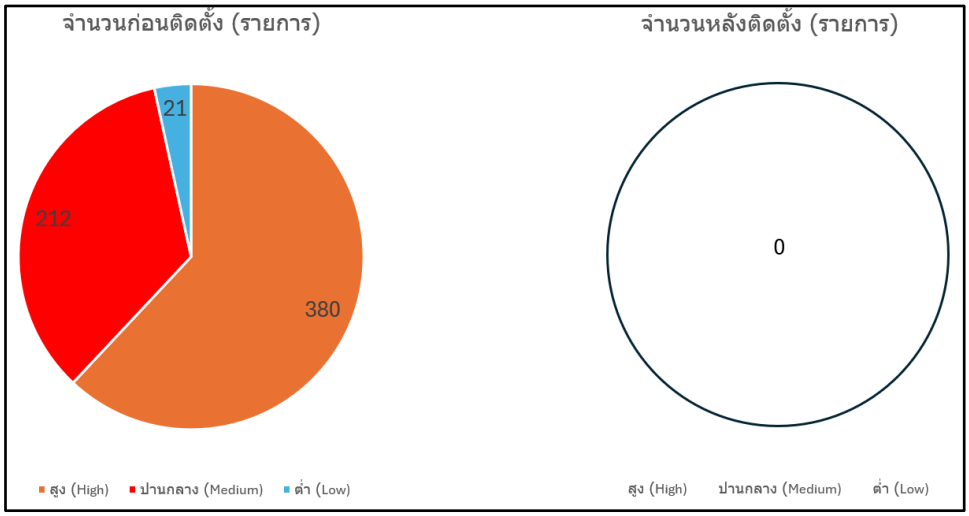
2. ผลการประเมินความสามารถในการลดช่องโหว่และรับมือภัยคุกคาม

จากการทดสอบในสภาพแวดล้อมจำลอง (Virtual Lab) พบว่าเฟรมเวิร์กสามารถยกระดับความปลอดภัยได้อย่างมีนัยสำคัญดังต่อไปนี้

2.1 การลดช่องโหว่ จากการสแกนระบบเพื่อค้นหาช่องโหว่ด้วยเครื่องมือ OpenVAS หลังการติดตั้งเฟรมเวิร์ก พบว่าจำนวนและความรุนแรงของช่องโหว่ลดลงอย่างมีนัยสำคัญ เมื่อเทียบกับผลการสแกนก่อนการติดตั้ง

ตารางที่ 2: เปรียบเทียบจำนวนช่องโหว่ที่ตรวจพบก่อนและหลังการติดตั้งเฟรมเวิร์ก เก็บข้อมูลระหว่างวันที่ 4 ตุลาคม 2568 ถึง 13 ตุลาคม 2568

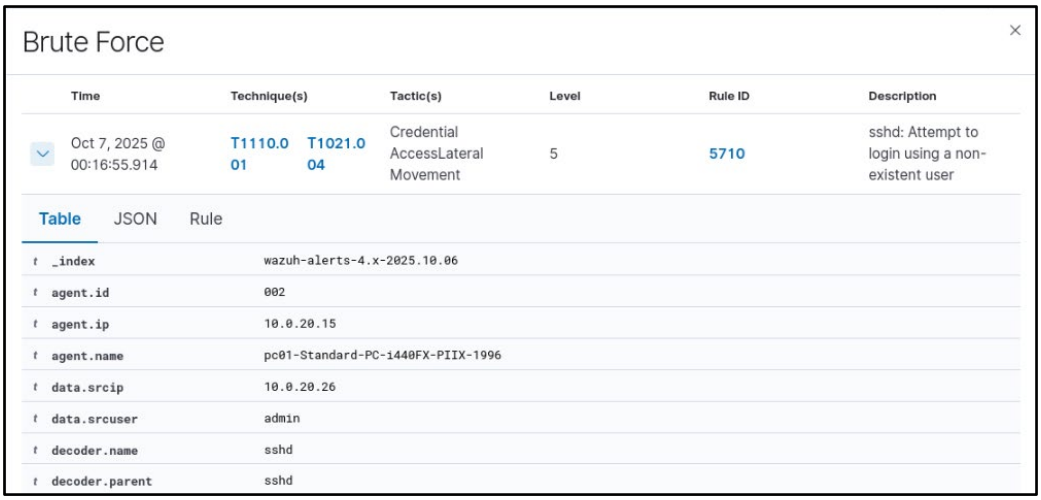
ระดับความรุนแรง (Severity)	จำนวนก่อนติดตั้ง (รายการ)	จำนวนหลังติดตั้ง (รายการ)	การลดลง (%)
สูง (High)	380	0	100%
ปานกลาง (Medium)	212	0	100%
ต่ำ (Low)	21	0	100%
รวมทั้งหมด	613	0	100%



รูปที่ 8: กราฟเปรียบเทียบจำนวนช่องโหว่ก่อนและหลังการติดตั้งเฟรมเวิร์ก

จากตารางที่ 2 และ รูปที่ 8 แสดงผลการเปรียบเทียบได้อย่างชัดเจน โดยก่อนการติดตั้งเฟรมเวิร์ก ตรวจพบช่องโหว่รวมทั้งสิ้น 613 รายการ แบ่งเป็นระดับความรุนแรง สูง (High) 380 รายการ, ปานกลาง (Medium) 212 รายการ และต่ำ (Low) 21 รายการ อย่างไรก็ตามภายหลังการติดตั้งเฟรมเวิร์ก ผลการสแกนไม่พบช่องโหว่ในทุกระดับความรุนแรง (0 รายการ) ซึ่งหมายความว่าช่องโหว่ทั้งหมดถูกแก้ไขและลดลง 100% ตามที่แสดงในตารางและกราฟวงกลมด้านขวา

2.2 การรับมือภัยคุกคาม ในสถานการณ์จำลองการโจมตี (Brute-force) ระบบสามารถ ตรวจจับและตอบสนองต่อภัยคุกคามได้อย่างทันท่วงที ซึ่งแสดงให้เห็นถึงประสิทธิภาพของเครื่องมืออย่าง Wazuh และการกำหนดค่าตาม SOPs ที่ออกแบบไว้



รูปที่ 9: การแจ้งเตือนlog บน Wazuh ขณะมีการพยายามสุ่มรหัสผ่าน (Brute-force)

จากรูปที่ 9 นี้จะแสดงหลักฐานว่าระบบสามารถตรวจจับ Rule ID: 5710 – sshd : Attempt to login using a non-existent user โดยระบุ IP ของผู้โจมตี, เป้าหมายที่ถูกโจมตี, และเวลาที่เกิดเหตุการณ์ ซึ่งยืนยันว่า Wazuh สามารถตรวจจับภัยคุกคามได้จริง

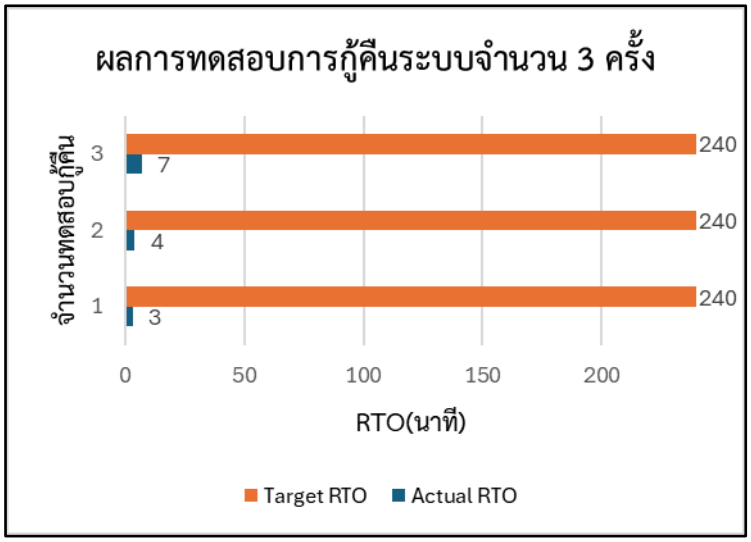
3. ผลการทดสอบความสามารถในการฟื้นตัวของระบบ (RTO)

เพื่อประเมินประสิทธิภาพของกระบวนการฟื้นคืนระบบ (System Recovery) ผู้วิจัยได้จำลองสถานการณ์ระบบล่มจากการโจมตีของแรนซัมแวร์ (Ransomware Attack) โดยมีสถานการณ์ทดสอบคือการกู้คืน Virtual Machine (VM) ที่มีความสำคัญ ขนาด 50GB ด้วย Proxmox Backup Server (PBS) ตามขั้นตอนที่ระบุไว้ในเอกสาร Runbook

ในการทดสอบนี้ ได้ตั้งค่าเป้าหมายเวลาในการกู้คืน (RTO) ไว้ที่ไม่เกิน 4 ชั่วโมง (240 นาที) ซึ่งมีเป้าหมายเวลาในการกู้คืน(RTO) ที่กำหนดไว้ไม่เกิน 4 ชั่วโมง ซึ่งเป็นเกณฑ์ที่ทางผู้เชี่ยวชาญประเมินว่ามีความเหมาะสม จากข้อคิดเห็นและข้อเสนอแนะจากผู้เชี่ยวชาญก่อนดำเนินการ ผลการทดสอบพบว่าระบบสามารถฟื้นคืนกลับมาให้บริการได้สำเร็จตามเป้าหมาย ซึ่งยืนยันถึงประสิทธิภาพของเฟรมเวิร์กในการรับมือและฟื้นตัวจากเหตุการณ์ไม่คาดฝัน โดยรายละเอียดของเวลาที่ใช้ในการกู้คืนจริงเมื่อเปรียบเทียบกับ Recovery Time Objective (RTO) เป้าหมาย แสดงดัง ตารางที่ 4 และ รูปที่ 8

ตารางที่ 3: ผลการทดสอบการกู้คืนระบบด้วย Proxmox Backup Server (PBS) จำนวน 3 ครั้ง

รอบที่	RTO	เวลาที่ใช้จริง (นาที)	ผลลัพธ์
1	4 ชั่วโมง	3	ผ่าน
2	4 ชั่วโมง	4	ผ่าน
3	4 ชั่วโมง	7	ผ่าน
ค่าเฉลี่ย	4 ชั่วโมง	4	ผ่าน



รูปที่ 10: กราฟเปรียบเทียบระหว่าง Target RTO และเวลาที่ Proxmox Backup Server (PBS) ทำได้จริง

จากการทดสอบทั้งหมด 3 ครั้ง พบว่าระบบสามารถกู้คืนได้สำเร็จทุกครั้ง โดยใช้เวลา 3 นาที, 4 นาที, และ 7 นาที ตามลำดับ ซึ่งเมื่อคำนวณเป็น ค่าเฉลี่ยแล้วจะอยู่ที่ 4 นาที

สรุปผลและอภิปรายผลการวิจัย

อาศัยแนวทาง Design Science Research (DSR) [33] ผสานร่วมกับมาตรฐาน NIST CSF 2.0 [17] แนวคิด Zero Trust และ Defense-in-Depth พร้อมบูรณาการเครื่องมือโอเพ่นซอร์ส [15], [26], [27], [28], [29], [30], [32] ในระบบ Proxmox VE [11], [12], [13] เพื่อลดต้นทุนและเพิ่มประสิทธิภาพการใช้งาน [5], [6], [23] ผลการประเมินโดยผู้เชี่ยวชาญ 5 ท่าน พบว่าเฟรมเวิร์กมีความเหมาะสมในระดับ มากถึงมากที่สุด โดยเฉพาะด้านนโยบายและ SOPs ที่ได้คะแนนเฉลี่ยสูงสุด (4.84) สะท้อนถึงความชัดเจนครอบคลุม และนำไปใช้ได้จริง ขณะที่ Runbooks (4.64) และ Form Templates (4.80) โดดเด่นในด้านการตอบสนองเหตุการณ์ฉุกเฉินและการจัดทำ Audit Trail อย่างมีระบบ นอกจากนี้การทดลองในสภาพแวดล้อมเสมือนจริงยังแสดงให้เห็นว่าเฟรมเวิร์กที่พัฒนาขึ้นสามารถลดจำนวนช่องโหว่และระยะเวลา Recovery Time Objective (RTO) ได้อย่างมีนัยสำคัญ [4], [21], [22], [24], [25] ตอบโจทย์ช่องว่างของงานวิจัยเดิมที่ยังขาดต้นแบบที่ครอบคลุมทั้งนโยบายกระบวนการ และเครื่องมือที่นำไปใช้ได้จริงสำหรับ SMEs

เมื่อเปรียบเทียบกับงานของ Grad [16], Patel and Schmidt [20] และ Chen et al. [2] พบว่าแนวคิดและแนวทางปฏิบัติของเฟรมเวิร์กที่นำเสนอมีความสอดคล้องอย่างชัดเจน โดยเฉพาะการจัดโครงสร้างตามฟังก์ชันของ NIST CSF และการประยุกต์ใช้ Zero Trust กับสภาพแวดล้อมระบบเสมือน อย่างไรก็ตามงานวิจัยนี้มีความแตกต่างจากงานของ Udroiu et al. [31] ที่เน้นการประเมินเชิงคุณภาพ และยังขาดการวิเคราะห์พฤติกรรมผู้ใช้งานตามแนวทาง User Behavior Modeling ซึ่งอาจเป็นทิศทางที่น่าสนใจในการขยายผลในอนาคต โดยสรุปเฟรมเวิร์กต้นแบบนี้มีศักยภาพสูงในการนำไปประยุกต์ใช้จริง โดยเฉพาะในองค์กรที่มีข้อจำกัดด้านทรัพยากร และสามารถต่อยอดสู่การพัฒนาเครื่องมืออัตโนมัติหรือการใช้ AI/ML ในระบบรักษาความมั่นคงปลอดภัยไซเบอร์ต่อไปได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะ

1. การขยายขอบเขตการประเมินประสิทธิภาพควรประเมินประสิทธิภาพของเฟรมเวิร์กในสภาพแวดล้อมที่มีความซับซ้อนสูงขึ้น เช่น Hybrid Cloud และ Multi-Cloud รวมถึงทดสอบความสามารถในการรับมือกับภัยคุกคามขั้นสูง (Advanced Persistent Threats - APTs) และการโจมตีแบบ Zero-Day

2. การบูรณาการเทคโนโลยีปัญญาประดิษฐ์ควรศึกษาและพัฒนาการนำ AI และ Machine Learning (ML) มาใช้ร่วมกับระบบ SIEM (Security Information and Event Management) เพื่อเพิ่มขีดความสามารถในการวิเคราะห์และตรวจจับภัยคุกคามเชิงรุก

3.การพัฒนาระบบตอบสนองอัตโนมัติควรพัฒนากลไกการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยอัตโนมัติ (SOAR) เพื่อลดระยะเวลาในการตอบสนอง (Incident Response Time) และเพิ่มประสิทธิภาพในการจัดการภัยคุกคาม

4.ข้อเสนอแนะเชิงประยุกต์องค์กรภาครัฐและเอกชน โดยเฉพาะกลุ่มธุรกิจขนาดกลางและขนาดย่อม (SMEs) สามารถนำผลการวิจัยไปปรับใช้เป็นกรอบการทำงานพื้นฐาน เพื่อยกระดับมาตรฐานความมั่นคงปลอดภัยไซเบอร์ขององค์กร

เอกสารอ้างอิง

[1] IBM, *"IBM X-Force 2025 Threat Intelligence Index,"* 2024. [Online]. Available: https://www.ibm.com/reports/threat-intelligence

[2] L. Chen, Y. Zhang, H. Li, and J. Wang, "A comparative analysis of cybersecurity frameworks for critical infrastructure protection," *J. Cybersecurity Privacy*, vol. 4, no. 2, pp. 205–220, 2024.

[3] D. Kumar and V. Gupta, "Improving cybersecurity of medical systems by applying the NIST framework," *Health Informatics J.*, vol. 29, no. 2, pp. 150–161, 2023.

[4] E. Babushkin, *"Automation of testing of operating system backup and recovery,"* M.S. thesis, Czech Technical Univ. Prague, Prague, Czech Republic, 2023.

[5] B. Dordevic, V. Timcenko, N. Kraljevic, and N. Jovicic, "Performance comparison of KVM and Proxmox type-1 hypervisors," in *Proc. 30th Telecommun. Forum (TELFOR)*, 2022, pp. 1–4, doi: 10.1109/TELFOR56187.2022.9983666.

[6] B. Dordevic, N. Kraljević, V. Timčenko, and N. Jovičić, "Performance comparison of KVM and Proxmox," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 1, pp. 35–44, 2024.

[7] Cybersecurity and Infrastructure Security Agency, *"ESXiArgs ransomware virtual machine recovery guidance,"* Feb. 8, 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-039a

[8] European Union Agency for Cybersecurity, *"ENISA Threat Landscape 2024,"* 2024. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[9] J. Manzoor, A. Waleed, A. F. Jamali, and A. Masood, "Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs," *PLOS ONE*, vol. 19, no. 3, Art. no. e0301183, 2024, doi: 10.1371/journal.pone.0301183.

[10] A. Alkhalifah, "Evaluating security and performance of open-source SIEM solutions for SMEs," *J. Inf. Secur. Appl.*, vol. 65, pp. 103–116, 2022.

[11] Proxmox Server Solutions GmbH, *"Proxmox Virtual Environment Administration Guide,"* ver. 8.3.1, 2024. [Online]. Available: https://www.proxmox.com

[12] Proxmox Server Solutions GmbH, *"Proxmox VE Datasheet,"* ver. 8.3, 2024. [Online]. Available: https://www.proxmox.com

[13] A. Simpalingabo, *"Comparison of Proxmox and OpenNebula as cyber range platforms,"* Cyber Defence Lab, Tech. Rep., 2024.

[14] P. Martinez and S. Garg, "Vulnerability management using open-source tools," *J. Inf. Syst. Secur.*, vol. 18, no. 1, pp. 55–68, 2022.

[15] N. Shivananjappa and R. Creutzburg, "Vulnerability management using open-source tools," *Electron. Imaging*, vol. 36, no. 3, Art. no. 326-1–326-8, 2024, doi: 10.2352/EI.2024.36.3.MOBMU-326.

[16] A. M. Grad, *"Nonprofit cybersecurity: NIST CSF 2.0 as exemplar of the zero-trust model,"* M.S. thesis, Univ. New Hampshire, Durham, NH, USA, 2024.

[17] National Institute of Standards and Technology, *"The NIST Cybersecurity Framework (CSF) 2.0,"* 2024, doi: 10.6028/NIST.CSWP.29.

[18] M. Parmar and A. Miles, "Cyber security frameworks (CSFs): An assessment between the NIST CSF v2.0 and EU standards," in *Proc. 2024 Security for Space Systems (3S)*, Noordwijk, Netherlands, 2024, pp. 1–7, doi: 10.23919/3S60530.2024.10592293.

[19] R. S. Perdana *et al.*, "Security and risk assessment of academic information systems using the NIST framework: A case study," in *Proc. 16th Int. Conf. Telecommun. Syst., Serv., Appl. (TSSA)*, 2022, pp. 1–5, doi: 10.1109/TSSA56819.2022.10063890.

[20] A. Patel and M. Schmidt, "Implementing zero trust in hybrid cloud environments," *IEEE Trans. Cloud Comput.*, vol. 12, no. 1, pp. 112–125, Jan. 2024.

[21] M. Kyryk *et al.*, "Disaster recovery solution for on-premises infrastructure using Proxmox Backup Server," in *Proc. IEEE 5th Int. Conf. Adv. Inf. Commun. Technol. (AICT)*, 2023, pp. 77–81, doi: 10.1109/AICT61584.2023.10452418.

[22] Proxmox Server Solutions GmbH, *"Proxmox Backup Server Documentation,"* ver. 3.3.0-1, 2024. [Online]. Available: https://www.proxmox.com

[23] Proxmox Server Solutions GmbH, *"Proxmox VE Ceph Benchmark,"* Dec. 11, 2023. [Online]. Available: https://www.proxmox.com

[24] Proxmox Server Solutions GmbH, *"Proxmox Backup Server Datasheet,"* ver. 3.3, 2024. [Online]. Available: https://www.proxmox.com

[25] A. A. Febriansyah and A. Prapanca, "Simulation of high-availability server implementation using Ceph on Proxmox," *J. Informatics Comput. Sci. (JINACS)*, vol. 6, no. 1, pp. 131–136, 2024, doi: 10.26740/jinacs.v6n01.p131-136.

[26] H. S. Abdullah, "Evaluation of open-source web application vulnerability scanners," *Acad. J. Nawroz Univ.*, vol. 9, no. 1, p. 47, 2020, doi: 10.25007/ajnu.v9n1a532.

[27] R. Pandey and S. Sharma, "Comparative study of open-source firewalls," *Int. J. Comput. Netw. Inf. Secur.*, vol. 13, no. 6, pp. 1–12, 2021.

[28] Netgate, *"pfSense Documentation,"* Sep. 19, 2025. [Online]. Available: https://docs.netgate.com/manuals/pfsense/en/latest/the-pfsense-documentation.pdf

[29] Greenbone Networks, *"Greenbone OpenVAS: Background and concepts,"* 2024. [Online]. Available: https://greenbone.github.io/docs/latest/background.html

[30] M. R. Islam and R. Rafique, "Wazuh SIEM for cybersecurity and threat mitigation in apparel industries," *Int. J. Eng. Mater. Manuf.*, vol. 9, no. 4, pp. 136–144, 2024, doi: 10.26776/ijemm.09.04.2024.02.

[31] A.-M. Udroiu, M. Dumitrache, and I. Sandu, "Open-source tools for the cybersecurity of an integrated information system," in *Proc. 14th Int. Conf. Electron., Comput. Artif. Intell. (ECAI)*, pp. 1–6, 2022.

[32] J.-Y. Seo *et al.*, "Real-time threat detection and prevention with Suricata, iptables, OSSEC, and the Elastic Stack," *J. Appl. Comput. Knowl.*, vol. 31, no. 2, pp. 1–8, 2024.

[33] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Q.*, vol. 28, no. 1, pp. 75–105, 2004, doi: 10.2307/25148625.