การพัฒนากระบวนการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัยของเครื่องแม่ข่าย คณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล

Development of a Security Information Management Processes and Server Security Events at Faculty of Science, Mahidol University

ปิยะนันต์ จำนงสุทธเสถียร[1*] และพิชิต ลีรุ่งนาวารัตน์[1]
Piyanan Jumnongsutthasatein[1*] and Pichit Leerungnavarat[1]

บทคัดย่อ

การให้บริการเว็บไซต์ของคณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล มีความเสี่ยงจากการโดนโจมตีทางไซเบอร์ และถูกบุกรุกเข้าสู่ระบบโดยไม่ได้รับอนุญาต จึงได้พัฒนากระบวนการจัดการข้อมูลด้านความปลอดภัยและเหตุการณ์ด้านความปลอดภัย (Security information and event management : SIEM) ของเครื่องแม่ข่าย คณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล โดยวิเคราะห์ปัญหาและอุปสรรคของกระบวนการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัยของเครื่องแม่ข่ายที่ให้บริการเว็บไซต์จำนวน 40 เครื่อง ที่ใช้ระบบปฏิบัติการและเว็บเซอร์วิสที่ต่างกันและศึกษาโปรแกรมประเภทโอเพนซอร์สที่มีความสามารถจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัยเพื่อนำมาพัฒนากระบวนการใหม่ พบว่าโปรแกรม Wazuh เป็นโปรแกรมประเภทโอเพนซอร์สที่มีความสามารถที่จะรวบรวมข้อมูลจราจรทางคอมพิวเตอร์จากเครื่องแม่ข่ายต่าง ๆ และนำมาวิเคราะห์ตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์แบบ Real-time เพื่อให้สามารถตอบสนองต่อเหตุการณ์ได้ทันท่วงที เช่น การปิดกั้นการเข้าถึงจากผู้ประสงค์ร้ายได้ และยังสามารถวิเคราะห์สืบสวนหาร่องรอยการโดนโจมตีในอดีตได้อีกด้วย จากการติดตั้ง ตั้งค่า ทดสอบประสิทธิภาพการทำงาน พบว่ากระบวนการทำงานใหม่มีการเก็บรวบรวมข้อมูลจราจรทางคอมพิวเตอร์มาทำการวิเคราะห์และตรวจสอบด้วยระบบอัตโนมัติแบบ Real-time สามารถค้นหาและคัดกรองข้อมูลเหตุการณ์ด้านความปลอดภัยที่ต้องการได้รวดเร็ว หากพบการโจมตีจะปิดกั้นโดยอัตโนมัติไม่ให้ผู้บุกรุกสามารถเข้าถึงเครื่องแม่ข่ายได้อีก รวมถึงโปรแกรมสามารถแสดงผลข้อมูลเหตุการณ์ด้านความปลอดภัยเป็นกราฟข้อมูลทางสถิติที่สามารถเข้าใจได้ง่าย อีกทั้งยังช่วยประหยัดงบประมาณค่าระบบจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัยได้หลายล้านบาทต่อปี

คำสำคัญ: การจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย
ความมั่นคงปลอดภัยทางไซเบอร์ ข้อมูลจราจรทางคอมพิวเตอร์

Abstract

Website service of the Faculty of Science, Mahidol University has a risk of being invaded by cyber-attacks and is being compromised into the system without permission. Therefore, a process for managing security information as well as security events (Security information and event management: SIEM) has been developed for the server of Faculty of Science, Mahidol University. SIEM has been developed by analyzing the problems and pain point of the security information management process and security incidents of 40 web servers running in different operating systems and web services and studying open-source applications capability of handling security data. It was found that the Wazuh, an open-source program has the ability to collect computer traffic data from various servers, as well as analyze and examine the computer traffic data in real-time. Wazuh can respond to security events in a timely manner, such as blocking access from malicious attackers. It can also analyze and investigate traces of attacks in the past as

[1] คณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล กรุงเทพมหานคร 10400
[1] Faculty of Science, Mahidol University, Bangkok 10400
*Corresponding author: e-mail: piyanan.jum@mahidol.ac.th
Received: *October 05, 2022*, Accepted: *January 05, 2023*, Published: *May 1, 2023*

well from installation, configuration, and performance testing. As a result, this new work process collects traffic data from computers to analyze and verify with a real-time automation. It offers a quick search feature with filtering options for retrieving security incident information. If an attack is detected, it will automatically block the attacker from accessing the server again. The system can also display safety event data as statistical graphs that can be easily understood. In addition, budget for the security information and security incidents management system has been reduced by millions of baht each year.

Keywords: data security and incidents management, cybersecurity, computer traffic data

บทนำ

งานสารสนเทศและห้องสมุดสตางค์ มงคลสุข คณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล มีภาระหน้าที่รับผิดชอบด้านเทคโนโลยีสารสนเทศของคณะ ได้แก่ รับผิดชอบเครื่องแม่ข่ายสำหรับให้บริการเว็บไซต์ หรือเว็บแอปพลิเคชันของภาควิชา ศูนย์ และหน่วยงานต่าง ๆ ภายในคณะ รวมถึงรับผิดชอบการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 ซึ่งงานสารสนเทศฯมีกระบวนการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์แบบปฐมภูมิ (Primary logging) คือ การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์บนตัวระบบที่สร้างข้อมูลนั้นขึ้นมาเอง (ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, 2560) อีกทั้งรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐาน ISO/IEC 27001:2013 มาตรฐานสากลสำหรับระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management Systems : ISMS) ในภาคผนวก A.16 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) (ภัทราพร, 2561) และตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ (ราชกิจจานุเบกษา, 2562) มาตรา 56 ว่าด้วยการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงการป้องกันและคุ้มครองข้อมูลส่วนบุคคลในระบบ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (ราชกิจจานุเบกษา, 2562) มาตรา 37 (1) ว่าด้วยการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 (ราชกิจจานุเบกษา, 2563) ข้อ 5 ว่าด้วยผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งควรครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (Administrative safeguard) มาตรการป้องกันด้านเทคนิค (Technical safeguard) และมาตรการป้องกันทางกายภาพ (Physical safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (Access control)

จากการให้บริการเว็บไซต์ของคณะวิทยาศาสตร์ พบว่ามีความเสี่ยงจากการโดนโจมตีทางไซเบอร์ และถูกบุกรุกเข้าสู่ระบบโดยไม่ได้รับอนุญาต เช่น การสแกนหาช่องโหว่ของเว็บ การพยายามเข้าระบบจัดการของ WordPress และการพยายามเข้าระบบผ่านทางโปรโตคอลต่าง ๆ เช่น SSH FTP SFTP เป็นต้น และการโจมตีเว็บแอปพลิเคชันด้วยเทคนิคและช่องโหว่ต่าง ๆ เช่น Broken Access Control, Injection, Identification and Authentication Failures, Vulnerable and Outdated Components, Security Logging and Monitoring Failures เป็นต้น (OWASP, 2021) สอดคล้องกับงานวิจัยของ Checkpoint (2022) ซึ่งรายงานว่าในไตรมาสที่ 2 ของปี ค.ศ. 2022 พบการโจมตีไปยังเป้าหมายที่เป็นกลุ่มธุรกิจด้านการศึกษาและวิจัยเพิ่มขึ้น 53% เมื่อเปรียบเทียบกับไตรมาสที่ 2 ของปี ค.ศ. 2021 และกลุ่มธุรกิจด้านการศึกษาและวิจัยยังเป็นกลุ่มที่โดนโจมตีเพิ่มขึ้นสูงที่สุดอีกด้วย รวมถึงเหตุข้อมูลส่วนบุคคลรั่วไหลจากองค์กรและบริษัทในไทยในปี ค.ศ. 2022 จากการโจมตีในรูปแบบ Ransomware โดยกลุ่มผู้ประสงค์ร้าย ALTDOS และกลุ่ม DESORDEN เพื่อนำข้อมูลไปขายในเว็บมืด (DISSENT, 2022) และการแพร่กระจายของ LockBit 2.0 ransomware (Bathgate, 2022) ซึ่งความเสี่ยงจากการโดนโจมตีทางไซเบอร์ดังกล่าว อาจก่อให้เกิดความเสียหายต่อข้อมูล ความต่อเนื่องทางธุรกิจ และชื่อเสียงของคณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล

การจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย (Security information and event management : SIEM) นิยามครั้งแรกโดยศูนย์วิจัย Gartner ในปี ค.ศ. 2005 (Williams and Nicolett, 2005) ว่า "SIEM technology provides real-time event management and historical analysis of security data from a wide set of heterogeneous sources. This technology is used to filter incident information into data that can be acted on for the purposes of incident response and forensic analysis." หมายถึง เทคโนโลยีที่สามารถจัดการเหตุการณ์ด้านความปลอดภัยแบบ Real-time และสามารถวิเคราะห์ประวัติข้อมูลด้านความปลอดภัยซึ่งมาจากแหล่งข้อมูลที่ต่างกันได้ ทั้งยังสามารถคัดกรองข้อมูลเหตุการณ์เพื่อนำมาใช้ตอบสนองต่อเหตุการณ์และวิเคราะห์สืบสวน ซึ่งคำว่า Security information and event management (SIEM) มาจากการผสมของ 2 การทำงานหลักที่ใช้ในการวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์บนระบบเครือข่าย คือ Security Event Management (SEM) คือ ระบบติดตามข้อมูลจราจรทางคอมพิวเตอร์ และ Security Information Management (SIM) คือ ระบบจัดเก็บ วิเคราะห์ และรายงานข้อมูลจราจรทางคอมพิวเตอร์ (Kakareka, 2014)

ในปัจจุบันความมั่นคงปลอดภัยทางไซเบอร์ถือเป็นส่วนที่สำคัญขององค์กร ในหลายองค์กรจึงมีการติดตั้งระบบจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย ใช้งานภายในศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operations Center : SOC) สำหรับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์เป็นหลัก งานสารสนเทศฯ จึงได้มีการศึกษาการจัดการข้อมูลด้านความปลอดภัยและเหตุการณ์ด้านความปลอดภัย เพื่อเพิ่มความสามารถในการรวบรวมและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ของเครื่องแม่ข่าย และเพื่อเฝ้าระวังและระงับเหตุที่อาจเกิดขึ้นได้

วัตถุประสงค์การวิจัย

1. เพื่อวิเคราะห์ปัญหาและอุปสรรคของการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย
2. เพื่อพัฒนากระบวนการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย
3. เพื่อทดสอบประสิทธิภาพของการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย
4. เพื่อประเมินผลการทำงานของกระบวนการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย

ระเบียบวิธีวิจัย

ขอบเขตการศึกษา

การวิจัยนี้เป็นงานวิจัยเชิงพัฒนามีขอบเขตการศึกษาและพัฒนากระบวนการจัดการข้อมูลด้านความปลอดภัยและเหตุการณ์ด้านความปลอดภัยของเครื่องแม่ข่ายที่ให้บริการเว็บไซต์ของคณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล ภายใต้การดูแลของงานสารสนเทศและห้องสมุดสตางค์ มงคลสุข จำนวน 40 เครื่อง ด้วยโปรแกรมประเภทโอเพนซอร์ส

ขั้นตอนและวิธีการดำเนินงาน

ขั้นตอนที่ 1 วิเคราะห์ปัญหาและอุปสรรคของการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย

1. ศึกษากระบวนการทำงานแบบเดิม และจัดทำรายการสินทรัพย์ (Asset inventory) ของเครื่องแม่ข่ายที่ให้บริการเว็บไซต์ของคณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล ภายใต้การดูแลของงานสารสนเทศและห้องสมุดสตางค์ มงคลสุข เช่น ข้อมูลระบบปฏิบัติการ ข้อมูลเว็บเซอร์วิส ข้อมูลการเก็บข้อมูลจราจรทางคอมพิวเตอร์ของแต่ละเครื่องแม่ข่าย
2. ศึกษาปัญหาเครื่องแม่ข่ายโดนโจมตีทางไซเบอร์
3. ศึกษาโปรแกรมประเภทโอเพนซอร์สที่มีความสามารถจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย

ขั้นตอนที่ 2 ออกแบบและพัฒนากระบวนการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย นำข้อมูลกระบวนการทำงานเดิม ปัญหาเครื่องแม่ข่ายโดนโจมตี และ ข้อมูลโปรแกรมจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัยมาออกแบบและพัฒนากระบวนการใหม่ ประกอบด้วย

1. กระบวนการติดตั้งโปรแกรมจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย
2. กระบวนการตั้งค่าการวิเคราะห์และตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์แบบ Real-time
3. กระบวนการตั้งค่าการปิดกั้นไม่ให้ผู้ที่พยายามบุกรุกเข้าถึงเครื่องแม่ข่าย

ขั้นตอนที่ 3 ทดสอบประสิทธิภาพของการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย ดำเนินการทดสอบประสิทธิภาพของกระบวนการทำงานใหม่เปรียบเทียบกับกระบวนการทำงานเดิม ดังนี้

1. ทดสอบจับเวลาที่ใช้ในการค้นหาข้อมูลจำนวนการเข้าเว็บไซต์ของหมายเลข IP 10.9.75.213 จากเครื่องแม่ข่ายจำนวน 40 เครื่อง ว่าใช้เวลาดำเนินการเท่าไร
2. ทดสอบการปิดกั้นไม่ให้ผู้ที่พยายามบุกรุกเข้าถึงเครื่องแม่ข่ายสำหรับทดสอบจำนวน 1 เครื่อง โดยการทดสอบเข้าสู่ระบบผ่านโปรโตคอล SSH ด้วยบัญชีที่ผิดซ้ำกัน 10 ครั้งติดต่อกัน ว่ามีการปิดกั้นหรือไม่ อย่างไร
3. ทดสอบการปิดกั้นไม่ให้ผู้ที่พยายามบุกรุกเข้าถึงเครื่องแม่ข่ายสำหรับทดสอบจำนวน 1 เครื่อง โดยการทดสอบเข้าสู่ระบบจัดการ WordPress ด้วยบัญชีที่ผิดซ้ำกัน 10 ครั้งติดต่อกัน ว่ามีการปิดกั้นหรือไม่ อย่างไร

ขั้นตอนที่ 4 ประเมินผลการทำงาน ประเมินผลการทำงานของกระบวนการใหม่เทียบกับกระบวนการเดิมในด้านประสิทธิภาพของการทำงานและระยะเวลาที่ใช้ในการทำงานต่าง ๆ ดังนี้

1. การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์การทำงานของเครื่องแม่ข่าย
2. การวิเคราะห์และตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์
3. การค้นหาข้อมูลเหตุการณ์ด้านความปลอดภัย
4. การปิดกั้นไม่ให้ผู้ที่พยายามบุกรุกเข้าถึงเครื่องแม่ข่าย
5. การแสดงข้อมูลเหตุการณ์ด้านความปลอดภัย

ผลการวิจัย

1. การวิเคราะห์ปัญหาและอุปสรรคของการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย

จากการศึกษากระบวนการทำงานแบบเดิม และจัดทำรายการสินทรัพย์ (Asset inventory) ของเครื่องแม่ข่ายที่ให้บริการเว็บไซต์ของคณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล ภายใต้การดูแลของงานสารสนเทศและห้องสมุดสตางค์ มงคลสุข พบว่ากระบวนการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัยบนเครื่องแม่ข่ายเดิม จะมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นแบบปฐมภูมิ และเครื่องแม่ข่ายจำนวน 40 เครื่อง ใช้ระบบปฏิบัติการที่แตกต่างกัน ได้แก่ Windows server และ Linux เครื่องแม่ข่ายใช้เว็บเซอร์วิสที่แตกต่างกัน ได้แก่ Apache HTTP, Nginx, OpenLite Speed, Apache Tomcat และ Internet Information Services (IIS) และไดเรกทอรีที่เก็บข้อมูลจราจรทางคอมพิวเตอร์แตกต่างกันตามการตั้งค่าของเว็บเซอร์วิส ประเภทข้อมูลจราจรทางคอมพิวเตอร์ที่มีการจัดเก็บ ได้แก่

- ข้อมูลจราจรทางคอมพิวเตอร์ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่าย (Access log)
- ข้อมูลจราจรทางคอมพิวเตอร์ที่มีการบันทึกไว้เมื่อมีการโอนแฟ้มข้อมูล
- ข้อมูลจราจรทางคอมพิวเตอร์ที่มีการบันทึกไว้เมื่อมีการใช้บริการเว็บ

ซึ่งกระบวนการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัยบนเครื่องแม่ข่ายเดิม มีปัญหาด้านประสิทธิภาพ

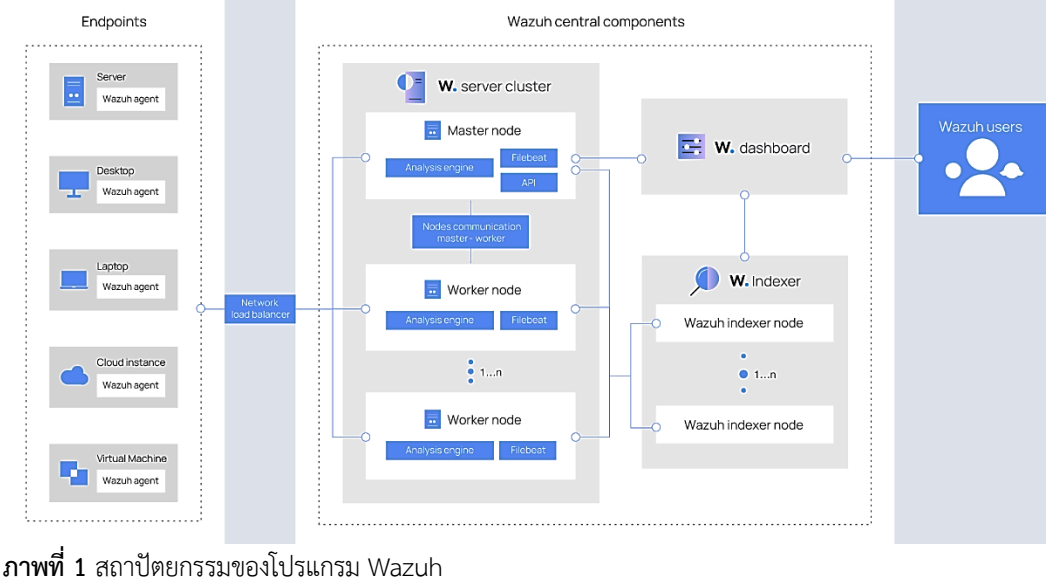
จากการศึกษาปัญหาเครื่องแม่ข่ายโดนโจมตีทางไซเบอร์ พบการโจมตีทางไซเบอร์ด้วยช่องทางต่าง ๆ ทั้งโจมตีที่ Web application หรือที่ Service หรือระบบปฏิบัติการของเครื่องเครื่องแม่ข่าย เช่น SQL Injection, Brute force attack, Scan port และ ช่องโหว่ Zero day ต่าง ๆ เช่น Shellshock, Heartbleed

จากการศึกษาโปรแกรมประเภทโอเพนซอร์สที่มีความสามารถจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย พบว่าโปรแกรม Wazuh มีความสามารถจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัยทั้งระบบปฏิบัติการ Windows server และ Linux สามารถตั้งค่าให้เก็บรวบรวมข้อมูลจราจรทางคอมพิวเตอร์จากไดเรกทอรีที่ต่างกันได้ และ สามารถตรวจสอบการโจมตีในรูปแบบต่าง ๆ ได้ อีกทั้งยังสามารถแสดงผลให้เข้าใจได้ง่าย

โปรแกรม Wazuh (Wazuh Inc., 2022) มีสถาปัตยกรรมที่ประกอบด้วยส่วนประกอบต่าง ๆ ดังนี้

1. Wazuh agent ติดตั้งลงบนเครื่องที่ต้องการจัดการ ทำหน้าที่ส่งข้อมูลจราจรทางคอมพิวเตอร์ให้ Wazuh server และมีหน้าที่สั่งให้ระบบปฏิบัติการปิดกั้นไม่ให้ผู้ที่พยายามบุกรุกเข้าถึงระบบบนเครื่องแม่ข่าย เมื่อได้รับคำสั่งจาก Wazuh server เรียกว่า Active Response
2. Wazuh server ทำหน้าที่วิเคราะห์และตรวจจับการโจมตีจากข้อมูลจราจรทางคอมพิวเตอร์ที่มาจาก Wazuh agents ประกอบด้วย Decoder คือ ถอดรหัสข้อมูลจราจรทางคอมพิวเตอร์ให้เป็นชุดข้อมูลที่สามารถนำมาวิเคราะห์ได้ และ Rules คือ กฎเกณฑ์สำหรับตรวจจับการโจมตีต่าง ๆ หากมีข้อมูลจราจรทางคอมพิวเตอร์ที่ตรงตาม Rules จะมีการแจ้งเตือนว่าเป็นการโจมตี และส่งให้ Wazuh indexer เก็บข้อมูลรายละเอียดข้อมูลนี้ไว้ต่อไป
3. Wazuh indexer คือส่วน Full-text search ทำหน้าที่จัดทำดัชนี จัดเก็บข้อมูลการแจ้งเตือนและข้อมูลเหตุการณ์ด้านความปลอดภัยที่สร้างโดย Wazuh server
4. Wazuh dashboard ทำหน้าที่แสดงข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัยแบบเว็บแอปพลิเคชันและเป็นเครื่องมือช่วยให้ผู้ใช้งานวิเคราะห์ข้อมูลได้สะดวก แบ่งเป็นด้านต่าง ๆ เช่น การจัดการข้อมูลด้านความปลอดภัย (Security information management) ช่องโหว่ที่พบ (Vulnerabilities)

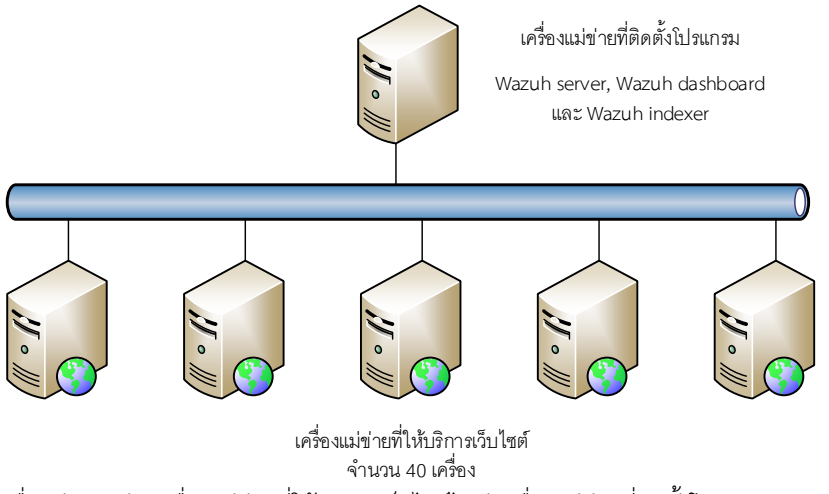
กระบวนการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของโปรแกรม Wazuh (ภาพที่ 1) เริ่มต้นที่ Wazuh agent บนเครื่องแม่ข่าย (Endpoints) เก็บข้อมูลจราจรทางคอมพิวเตอร์ของแต่ละเครื่องแล้วส่งต่อให้ Wazuh server นำมาวิเคราะห์ข้อมูล ถอดรหัส และตรวจจับการโจมตี แล้วจึงจัดเก็บข้อมูลการแจ้งเตือนและข้อมูลเหตุการณ์ด้านความปลอดภัยลงบน Wazuh indexer และทั้ง Wazuh server และ Wazuh indexer จะเชื่อมต่อกับส่วนติดต่อผู้ใช้งาน Wazuh dashboard สำหรับแสดงผลการทำงานแก่ผู้ใช้งาน



ภาพที่ 1 สถาปัตยกรรมของโปรแกรม Wazuh

2. ออกแบบและพัฒนากระบวนการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย

ผลจากการวิเคราะห์ปัญหาและอุปสรรคของการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย ผู้วิจัยจึงได้ออกแบบกระบวนการและนำเครื่องมือเข้ามาจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย โดยให้โปรแกรม Wazuh server, Wazuh dashboard และ Wazuh indexer ทำงานอยู่บนเครื่องแม่ข่ายใหม่ และให้ Wazuh agent อยู่บนเครื่องแม่ข่ายที่ให้บริการเว็บไซต์ ทำหน้าที่เก็บรวบรวมข้อมูลจราจรทางคอมพิวเตอร์จากเครื่องแม่ข่ายต่าง ๆ ส่งมาให้โปรแกรม Wazuh server นำมาประมวลผลต่อไปตามภาพที่ 2



ภาพที่ 2 การเชื่อมต่อระหว่างเครื่องแม่ข่ายที่ให้บริการเว็บไซต์ไปยังเครื่องแม่ข่ายที่ติดตั้งโปรแกรม Wazuh server

การออกแบบให้มีกระบวนการในการพัฒนาดังนี้

2.1. กระบวนการติดตั้งโปรแกรม Wazuh server, Wazuh dashboard และ Wazuh indexer ลงบนเครื่องแม่ข่ายที่สร้างใหม่สำหรับประมวลผล พร้อมทั้งตั้งค่าโปรแกรม และตั้งค่าการป้องกันของเครื่องแม่ข่ายแล้ว

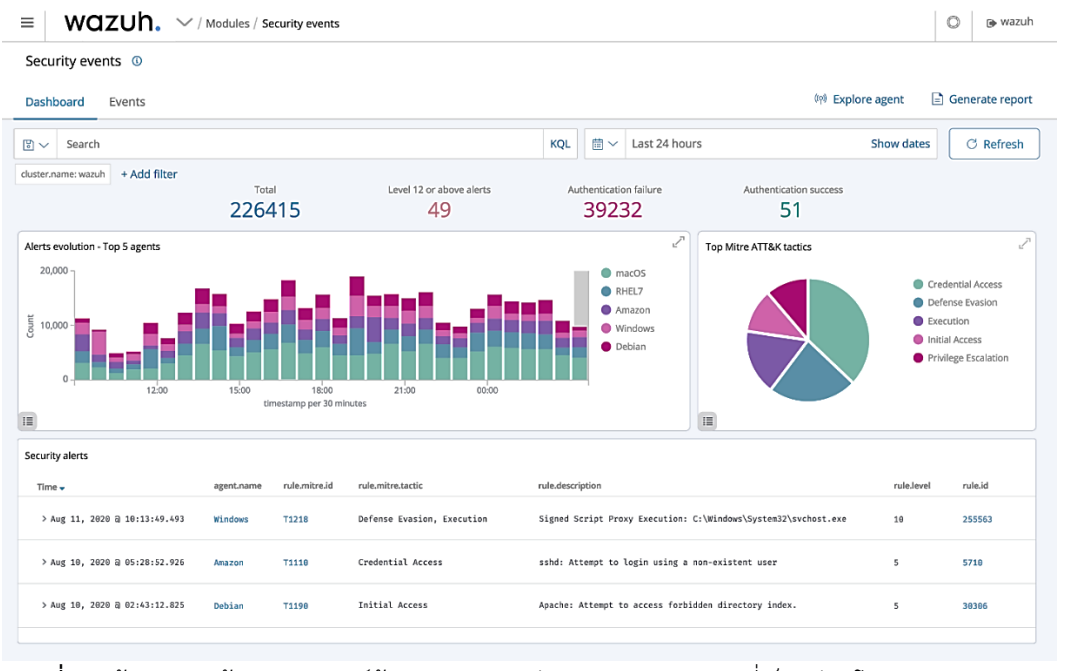
2.2. กระบวนการติดตั้ง Wazuh agent ลงบนเครื่องแม่ข่ายที่ให้บริการเว็บไซต์ของคณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล จำนวน 40 เครื่อง พร้อมทั้งตั้งค่ากำหนดไดเรกทอรีและไฟล์ข้อมูลจราจรทางคอมพิวเตอร์ที่ต้องการ ซึ่งแตกต่างกันไปตามแต่ละเครื่องแม่ข่าย เช่น ไฟล์ข้อมูลจราจรทางคอมพิวเตอร์อยู่ที่ไดเรกทอรี C:\Windows\app และ IIS ตั้งชื่อไฟล์ตามวันที่เก็บ จึงต้องเพิ่มการตั้งค่า ดังนี้

```
<localfile>
  <location>C:\Windows\app\log-%y-%m-%d.log</location>
  <log_format>syslog</log_format>
</localfile>
```

2.3. กระบวนการตั้งค่าการวิเคราะห์และตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์แบบ Real-time ได้แก่ การตั้งค่า Decoder ให้สามารถถอดรหัสจากข้อมูลจราจรของเว็บเซอร์วิสต่าง ๆ เช่น IIS บน Windows server ได้

2.4. กระบวนการตั้งค่าการปิดกั้นไม่ให้ผู้ที่พยายามบุกรุกเข้าถึงเครื่องแม่ข่าย ได้แก่ การตั้งค่า Rules และตั้งค่า Active Response เพิ่มเงื่อนไขให้มีการปิดกั้นเมื่อมีผู้ประสงค์ร้ายพยายามเข้าสู่ระบบบนเครื่องแม่ข่าย โดยอ้างอิงจากผลการศึกษาปัญหาเครื่องแม่ข่ายโดนโจมตี เช่น SQL Injection, Brute force attack, Scan port และ ช่องโหว่ Zero day ต่าง ๆ เช่น Shellshock, Heartbleed

ภายหลังเสร็จสิ้นกระบวนการติดตั้ง เมื่อเข้าสู่ระบบ Wazuh dashboard จะแสดงข้อมูลเหตุการณ์ด้านความปลอดภัยที่ได้รับจาก Wazuh agent และกราฟแสดงสถิติที่มีการจัดเก็บดังภาพที่ 3



ภาพที่ 3 หน้าจอแสดงข้อมูลเหตุการณ์ด้านความปลอดภัยและกราฟแสดงสถิติที่เก็บอยู่บนโปรแกรม Wazuh

3. ทดสอบประสิทธิภาพของการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย

3.1. การทดสอบจับเวลาที่ใช้ในการค้นหาข้อมูลจำนวนการเข้าเว็บไซต์ของหมายเลข IP 10.9.75.213 จากเครื่องแม่ข่ายจำนวน 40 เครื่อง

กระบวนการเดิมจะทำการวิเคราะห์และตรวจสอบด้วยบุคลากร ตั้งแต่ค้นหาไฟล์ข้อมูลจราจรทางคอมพิวเตอร์ที่เก็บไว้บนเครื่องแม่ข่าย และคัดลอกไฟล์จากเครื่องแม่ข่ายทั้ง 40 เครื่องมาไว้ในเครื่องคอมพิวเตอร์เครื่องเดียวกัน เปิดไฟล์ทั้ง 40 ไฟล์ ด้วยเมนู Append Access Log บนโปรแกรม Apache http Logs Viewer แล้วเลือกกรองข้อมูลด้วย IP 10.9.75.213 ใช้เวลาประมาณ 3 ชั่วโมง 30 นาที กระบวนการใหม่ค้นหาผ่านระบบ Wazuh dashboard เข้าเมนู Security events เลือก Add filter ใส่ค่า data.src_ip is 10.9.75.213 ใช้เวลาประมาณ 3 นาที

3.2. ทดสอบการปิดกั้นไม่ให้ผู้ที่พยายามบุกรุกเข้าถึงเครื่องแม่ข่ายตัวสำหรับทดสอบจำนวน 1 เครื่อง โดยการทดสอบเข้าสู่ระบบผ่านโปรโตคอล SSH ด้วยบัญชีที่ผิดซ้ำกัน 10 ครั้งติดต่อกัน

หลังจากการทดสอบพยายามเข้าระบบผิดพลาดติดต่อกัน พบว่าไม่สามารถเชื่อมต่อเครื่องแม่ข่ายสำหรับทดสอบได้หลังจากการพยายามเข้าครั้งที่ 5 เนื่องจากโปรแกรม Fail2ban ที่ติดตั้งบนเครื่องแม่ข่ายสำหรับทดสอบทำการปิดกั้นเมื่อเข้าสู่ระบบผิดพลาดเกินจำนวนที่กำหนด และพบว่าโปรแกรม Wazuh ได้เก็บข้อมูลเหตุการณ์ด้านความปลอดภัยว่ามีการเข้าสู่ระบบผิดพลาดจำนวน 5 ครั้ง

3.3. ทดสอบการปิดกั้นไม่ให้ผู้ที่พยายามบุกรุกเข้าถึงเครื่องแม่ข่ายสำหรับทดสอบจำนวน 1 เครื่อง โดยการทดสอบเข้าสู่ระบบจัดการ WordPress ด้วยบัญชีที่ผิดซ้ำกัน 10 ครั้งติดต่อกัน

หลังจากการทดสอบพยายามเข้าระบบผิดพลาดติดต่อกัน พบว่าไม่สามารถเชื่อมต่อเครื่องแม่ข่ายสำหรับทดสอบได้หลังจากการพยายามเข้าครั้งที่ 8 เนื่องจากโปรแกรม Wazuh ตรวจจับข้อมูลเหตุการณ์ด้านความปลอดภัยว่ามีการเข้าสู่ระบบผิดพลาดจำนวน 8 ครั้ง ตามการตั้งค่าใน Rules จึงส่งคำสั่ง Active Response ให้เครื่องแม่ข่ายสำหรับทดสอบปิดกั้นการเข้าถึงจากผู้ที่พยายามบุกรุก

4. ประเมินผลการทำงาน

ผลการเปรียบเทียบกระบวนการทำงานเดิมของการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัยของเครื่องแม่ข่าย กับกระบวนการทำงานใหม่ที่พัฒนาขึ้นมีรายละเอียด ดังตารางที่ 1

ตารางที่ 1 การเปรียบเทียบกระบวนการทำงานเดิมและกระบวนการใหม่ของการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัยของเครื่องแม่ข่าย

กระบวนการทำงาน	กระบวนการเดิม	กระบวนการใหม่
การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์การทำงานของเครื่องแม่ข่าย	เก็บอยู่บนเครื่องแม่ข่ายที่สร้างข้อมูลนั้นขึ้นมาเอง	เก็บอยู่บนเครื่องแม่ข่ายของแต่ละเครื่อง และนำมาวิเคราะห์ ตรวจสอบ และเก็บข้อมูลเหตุการณ์ด้านความปลอดภัยไว้ที่โปรแกรม Wazuh ด้วย
การวิเคราะห์และตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์	ไม่มี	ทำการวิเคราะห์และตรวจสอบด้วยระบบอัตโนมัติแบบ Real-time บน โปรแกรม Wazuh ใช้เวลา 1-2 นาที นับตั้งแต่เกิดข้อมูลจราจรทางคอมพิวเตอร์ ผ่านการวิเคราะห์และตรวจจับการโจมตี และจัดเก็บข้อมูลการแจ้งเตือนและข้อมูลเหตุการณ์ด้านความปลอดภัยไปยัง Wazuh indexer
การค้นหาข้อมูลเหตุการณ์ด้านความปลอดภัย	ค้นหาด้วย Apache http logs viewer ด้วยบุคลากรใช้เวลาประมาณ 3 ชั่วโมง 30 นาที	ค้นหาและคัดกรองข้อมูลที่ต้องการได้ผ่านโปรแกรม Wazuh dashboard ใช้เวลาประมาณ 3 นาที
การปิดกั้นไม่ให้ผู้ที่พยายามบุกรุกเข้าถึงเครื่องแม่ข่าย	ตั้งค่าการปิดกั้นอัตโนมัติด้วยโปรแกรม Fail2ban บนโปรโตคอล SSH, FTP และ SFTP ปิดกั้นเมื่อเข้าสู่ระบบผิดพลาดเกินจำนวนที่กำหนด	ตั้งค่าการปิดกั้นอัตโนมัติด้วยโปรแกรม Fail2ban และ Active Response ของ Wazuh บนโปรโตคอล SSH, FTP, SFTP และ HTTPS ปิดกั้นเมื่อเข้าสู่ระบบผิดพลาดเกินจำนวนที่กำหนด หรือ ตามการตั้งค่า เช่น เข้าระบบ WordPress ผิดพลาด, ใช้โปรแกรม Zgrab ค้นหาช่องโหว่ของระบบ
การแสดงข้อมูลเหตุการณ์ด้านความปลอดภัย	แสดงผลเป็นไฟล์ข้อมูลจราจรทางคอมพิวเตอร์แยกเป็นไฟล์ต่าง ๆ ตามการตั้งค่าบนเครื่องแม่ข่าย	แสดงผลเป็นกราฟข้อมูลทางสถิติ และข้อมูลจราจรทางคอมพิวเตอร์ที่เป็นข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัยที่ผ่านการวิเคราะห์และตรวจสอบแล้ว

สรุปผลการวิจัย

การพัฒนากระบวนการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัยของเครื่องแม่ข่าย ด้วยการประยุกต์ใช้งานโปรแกรมประเภทโอเพนซอร์ส Wazuh นี้ สามารถพัฒนากระบวนการทำงานให้เป็นระบบ และมีประสิทธิภาพ ทั้งการวิเคราะห์และตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ต่าง ๆ บนเครื่องแม่ข่ายจำนวน 40 เครื่อง ที่ใช้ระบบปฏิบัติการและเว็บเซอร์วิสที่ต่างกัน และมีปัญหาการโดนโจมตีทางไซเบอร์ด้วยช่องทางต่าง ๆ โดยขั้นตอนการติดตั้งโปรแกรม Wazuh จะต้องมีการตั้งค่าให้เหมาะสมกับสภาพแวดล้อมของเครื่องแม่ข่ายที่ต่างกัน เช่น ตั้งค่าไดเรกทอรีที่เก็บข้อมูลจราจรทางคอมพิวเตอร์, ตั้งค่า Decoder, ตั้งค่า Rules และตั้งค่า Active Response ให้สามารถทำงานได้อย่างมีประสิทธิภาพและครอบคลุมการทำงานของเครื่องแม่ข่ายทั้ง 40 เครื่อง จากการทดสอบพบว่ากระบวนการใหม่มีการรวบรวม วิเคราะห์ และตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ด้วยโปรแกรม Wazuh แบบอัตโนมัติ และทำงานแบบ Real-time สามารถค้นหาและคัดกรองข้อมูลเหตุการณ์ด้านความปลอดภัยที่ต้องการได้อย่างรวดเร็ว รวมถึงปิดกั้นไม่ให้ผู้ที่พยายามบุกรุกเข้าถึงเครื่องแม่ข่ายได้เป็นอย่างดี พร้อมทั้งแสดงข้อมูลเหตุการณ์ด้านความปลอดภัยออกมาเป็นกราฟข้อมูลทางสถิติที่สามารถเข้าใจได้ง่าย

อภิปรายผลการวิจัยและข้อเสนอแนะ

การศึกษาและพัฒนากระบวนการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัยของเครื่องแม่ข่าย คณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล โดยเริ่มจากการศึกษาปัญหาและอุปสรรคของการจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัย พบว่าเครื่องแม่ข่ายจำนวน 40 เครื่อง เก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้บนเครื่องตัวเอง และเครื่องแม่ข่ายยังมีระบบปฏิบัติการที่แตกต่างกัน มีเว็บเซอร์วิสและพื้นที่จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไม่เหมือนกันในทุกเครื่อง รวมถึงปัญหาการโดนโจมตีทางไซเบอร์อย่างต่อเนื่องและมีแนวโน้มทวีความรุนแรง จึงได้ทำการศึกษา ออกแบบและพัฒนากระบวนการจัดการข้อมูลด้าน

ความปลอดภัย และเหตุการณ์ด้านความปลอดภัยของเครื่องแม่ข่ายด้วยโปรแกรม Wazuh ซึ่งติดตั้งได้ง่ายและมีความสามารถมากกว่าระบบค้นหาข้อมูลจราจรทางคอมพิวเตอร์ด้วยวิธี Map/Reduce บนกรอบการทำงานของ Hadoop ของชูพันธุ์ (2555) เมื่อติดตั้งและตั้งค่าโปรแกรมเสร็จจึงทำการทดสอบประสิทธิภาพให้ระบบสามารถทำงานสอดคล้องร่วมกันกับเครื่องแม่ข่ายให้กระบวนการมีความสมบูรณ์ และมีประสิทธิภาพที่ดีกว่ากระบวนการทำงานเดิม สามารถที่จะรวบรวมข้อมูลจราจรทางคอมพิวเตอร์จากเครื่องแม่ข่ายต่าง ๆ และนำมาวิเคราะห์ตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์แบบ Real-time เพื่อให้สามารถตอบสนองต่อเหตุการณ์ได้ทันท่วงที เพิ่มการดูแลเฝ้าระวังและป้องกันภัยไซเบอร์ที่มีแนวโน้มการโจมตีเข้ามายังเครื่องแม่ข่ายเพิ่มขึ้นทุกปีได้เป็นอย่างดี ช่วยป้องกันเหตุข้อมูลส่วนบุคคลรั่วไหลจากการโดนโจมตี และยังสามารถวิเคราะห์สืบสวนหาร่องรอยการโดนโจมตีในอดีตได้อีกด้วย กระบวนการที่พัฒนาขึ้นมาใหม่นี้มีประสิทธิภาพ ลดภาระและขั้นตอนการทำงานที่อาศัยมนุษย์ และจากการใช้โปรแกรมประเภทโอเพนซอร์สทำให้ช่วยประหยัดงบประมาณค่าระบบจัดการข้อมูลด้านความปลอดภัย และเหตุการณ์ด้านความปลอดภัยได้หลายล้านบาทต่อปี

ทั้งนี้การป้องกันการโจมตีทางไซเบอร์ให้ได้ผลที่ดีนั้นยังคงต้องอาศัยส่วนประกอบอีกหลายส่วนตามข้อเสนอและมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (2557) ระบุไว้สี่หมวดว่า (1) การวางแผน (Planning) ประกอบด้วยแนวทางในการวางแผนบริหารจัดการเว็บไซต์ซึ่งได้แก่ การวางแผนด้านความมั่นคงปลอดภัยของเว็บไซต์แนวทางการเลือกผู้รับจดทะเบียนชื่อโดเมน แนวทางการเลือกผู้ให้บริการเว็บโฮสติ้ง และ แนวทางในการเลือกใช้ระบบบริหารจัดการเว็บไซต์ (Content Management System: CMS) (2) การติดตั้งและการตั้งค่าที่เกี่ยวข้องกับเว็บไซต์ (Installation and Configuration) เป็นข้อกำหนดที่มุ่งเน้นให้มีการติดตั้งและการตั้งค่าของ โปรแกรมสำหรับให้บริการเว็บ ระบบบริหารจัดการเว็บไซต์ ระบบฐานข้อมูล และ Server-Side Script Engine รวมถึงแนวทางการกำหนดรหัสผ่านที่มั่นคงปลอดภัย (3) การพัฒนาโปรแกรมประยุกต์บนเว็บอย่างมั่นคงปลอดภัย ซึ่งข้อกำหนดในส่วนนี้เน้นการป้องกันการโจมตีด้วยเทคนิคต่าง ๆ ที่พบบ่อยจากรายงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือไทยเซิร์ต (ThaiCERT) แนวทางการป้องกันจากเอกสารของ IPA และ OWASP (4) การรับมือเหตุภัยคุกคาม (Security Incident Handling) เป็นข้อกำหนดที่มุ่งเน้นให้ผู้ดูแลเครื่องบริการเว็บสามารถรับมือกับเหตุภัยคุกคามด้านความมั่นคงปลอดภัยที่เกิดขึ้นกับเว็บไซต์ได้แก่ กรณีเว็บไซต์ถูกบุกรุกและควบคุม (Intrusions) กรณีการถูกโจมตีในลักษณะ (Denial of Services: DoS) และ กรณีโดเมนถูกขโมย (Domain Hijack) เป็นต้น

ข้อเสนอแนะการวิจัย

โปรแกรม Wazuh ยังมีความสามารถอื่น ๆ เกี่ยวกับด้านความปลอดภัยทางไซเบอร์ เช่น Security configuration assessment คือ การตรวจสอบการตั้งค่าตามมาตรฐานความปลอดภัยของระบบปฏิบัติการนั้น ๆ และ Vulnerability คือ การตรวจสอบช่องโหว่ที่มีการเผยแพร่ออกมา ซึ่งสามารถนำมาใช้เพื่อการบริหารความเสี่ยงทางเทคโนโลยีสารสนเทศให้ปลอดภัยได้ดียิ่งขึ้น และสามารถนำไปพัฒนาต่อยอดจัดตั้งศูนย์ปฏิบัติการไซเบอร์เพื่อเฝ้าระวังภัยคุกคาม (Security Operations Center : SOC หรือ Cyber Security Operations Center : CSOC) เพื่อเป็นศูนย์กลางในการเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์ขององค์กรต่อไป

กิตติกรรมประกาศ

งานวิจัยนี้สำเร็จลุล่วงได้ด้วยดีด้วยความกรุณาของคุณวรัษยา สุนทรศารทูล ผู้ช่วยคณบดีฝ่ายการเปลี่ยนผ่านสู่ระบบดิจิทัล และคุณเฉิดฉันทร์ ราชบุรณะ หัวหน้างานสารสนเทศและห้องสมุดสตางค์ มงคลสุข คณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล รวมถึงคณะผู้ทรงคุณวุฒิ และบรรณาธิการวารสารวิชาการ ปขมท. ที่ให้ความกรุณาตรวจทานและแก้ไขบทความฉบับนี้จนเสร็จสมบูรณ์ ทางผู้วิจัยขอกราบขอบพระคุณไว้ ณ โอกาสนี้

เอกสารอ้างอิง

ชูพันธุ์ รัตนโภคา. 2555. การออกแบบและพัฒนาระบบค้นหาข้อมูลจราจรทางคอมพิวเตอร์ด้วยวิธี Map/Reduce บนกรอบการทำงานของ Hadoop. วารสารวิชาการเทคโนโลยีอุตสาหกรรม. 8(3): 18-27.

ภัทราพร โชติมหา. 2561. การจัดทำแนวทางการตรวจสอบภายในตามมาตรฐาน ISO 27001 : 2013 กรณีศึกษาการทางพิเศษแห่งประเทศไทย. หน้า 286-295. *ใน:* การประชุมวิชาการระดับชาติและนานาชาติ. วันที่ 12 กรกฎาคม พ.ศ. 2561. มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี.

ราชกิจจานุเบกษา. 2562. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. 32 หน้า.

ราชกิจจานุเบกษา. 2562. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. 44 หน้า.

ราชกิจจานุเบกษา. 2563. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563. 2 หน้า.

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. 2560. มาตรฐานศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ เล่ม 1 ข้อกำหนด. 30 หน้า.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. 2557. ข้อเสนอและมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์. 53 หน้า.

Kakareka, A. 2014. Detecting System Intrusions. Pages 1-27. *In:* John R. Vacca. (ed). Network and System Security (Second Edition). Syngress. 406 pages.

Check Point Blog. 2022. Check Point Research: Weekly Cyber Attacks increased by 32% Year-Over-Year; 1 out of 40 organizations impacted by Ransomware. [Online]. Available: https://blog.checkpoint.com/2022/07/26/check-point-research-weekly-cyber-attacks-increased-by-32-year-over-year-1-out-of-40-organizations-impacted-by-ransomware-2/. (Retrieved October 2022).

DISSENT. 2022. Thai entities continue to fall prey to cyberattacks and leaks. [Online]. Available: https://www.databreaches.net/thai-entities-continue-to-fall-prey-to-cyberattacks-and-leaks/. (Retrieved November 2022).

OWASP. 2021. OWASP Top Ten. [Online]. Available: https://owasp.org/www-project-top-ten/. (Retrieved November 2022).

Rory Bathgate. 2022. LockBit 2.0 ransomware disguised as PDFs distributed in email attacks. [Online]. Available: https://www.itpro.com/security/368363/lockbit-20-ransomware-disguised-as-pdfs-distributed-in-email-attacks. (Retrieved November 2022).

Wazuh Inc. 2022. Wazuh Documentation. [Online]. Available: https://documentation.wazuh.com/current/index.html. (Retrieved November 2022).

Williams A. and M. Nicolett. 2005. Improve IT security with vulnerability management. Gartner – technical report (ID: G00127481).