

การพัฒนาระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์
แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์
ตอบสนองต่อภัยคุกคามแบบเรียลไทม์

**DEVELOPING CYBER THREAT PREVENTION AND ALERT SYSTEMS
ON THE SERVER USING REAL-TIME THREAT RESPONSE EVENT
ANALYSIS TECHNIQUES**

กฤษ ศรีเงินดี

KIT SRINGENDEE

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
ปีการศึกษา 2566
ลิขสิทธิ์ของมหาวิทยาลัยศรีปทุม

การพัฒนาระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์
แม้ข้ามโดยใช้เทคนิคการวิเคราะห์เหตุการณ์
ตอบสนองต่อภัยคุกคามแบบเรียลไทม์

กฤษ ศรีเงินดี

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
ปีการศึกษา 2566
ลิขสิทธิ์ของมหาวิทยาลัยศรีปทุม

**DEVELOPING CYBER THREAT PREVENTION AND ALERT SYSTEMS
ON THE SERVER USING REAL-TIME THREAT RESPONSE EVENT
ANALYSIS TECHNIQUES**

KIT SRINGENDEE

**A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY
SCHOOL OF INFORMATION TECHNOLOGY
SRIPATUM UNIVERSITY
ACADEMIC YEAR 2023
COPYRIGHT OF SRIPATUM UNIVERSITY**

ชื่อหัวข้อวิทยานิพนธ์

การพัฒนาระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์
บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์
เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์
DEVELOPING CYBER THREAT PREVENTION AND
ALERT SYSTEMS ON THE SERVER USING
REAL-TIME THREAT RESPONSE EVENT ANALYSIS
TECHNIQUES

นักศึกษา

นายกฤษ ศรีเงินดี รหัสประจำตัว 66501988

หลักสูตร

วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะ

เทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

อาจารย์ที่ปรึกษาวิทยานิพนธ์

ผู้ช่วยศาสตราจารย์ ดร.สุรศักดิ์ มั่งสิงห์

อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

ศาสตราจารย์ ดร.ประสงค์ ปรานีตพลกรัง

คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่ง
ของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ


.....คณบดีคณะเทคโนโลยีสารสนเทศ
(ผู้ช่วยศาสตราจารย์ ดร.ปราณี มณีรัตน์)
วันที่ ๒ เดือน ๓ พ.ศ. ๖๗



คณะกรรมการสอบวิทยานิพนธ์


.....ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ก้องกาญจน์ สุขคณาภิบาล)


.....กรรมการ (ผู้ช่วยศาสตราจารย์ ดร.พชีพ ศรีนาม)


.....กรรมการ (ผู้ช่วยศาสตราจารย์ ดร.สุรศักดิ์ มั่งสิงห์)


.....กรรมการ
(ศาสตราจารย์ ดร.ประสงค์ ปรานีตพลกรัง)

วิทยานิพนธ์เรื่อง	การพัฒนาระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์
คำสำคัญ	ภัยคุกคามทางไซเบอร์, การป้องกันภัยคุกคามทางไซเบอร์, การแจ้งเตือนภัยคุกคามทางไซเบอร์
นักศึกษา	นายกฤษ ศรีเงินดี รหัสประจำตัว 66501988
อาจารย์ที่ปรึกษา	ผู้ช่วยศาสตราจารย์ ดร.สุรศักดิ์ มั่งสิงห์
อาจารย์ที่ปรึกษาร่วม	ศาสตราจารย์ ดร.ประสงค์ ปรานีตพลกรัง
หลักสูตร	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะ	เทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
ปีการศึกษา	2566

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์ 1) เพื่อทำการวิเคราะห์ภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายในองค์กร 2) พัฒนาระบบป้องกัน และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ 3) เพื่อทำการประเมินประสิทธิภาพของระบบป้องกัน และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย 4) นำเสนอแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ใหม่ที่เหมาะสมกับองค์กร ภายใต้ฐานความคิดที่ไม่ไว้วางใจใคร หากแต่ต้องตรวจสอบอยู่เสมอ ทั้งนี้ การวิจัยได้ทำอยู่ใน 2 ส่วน คือ ส่วนที่ 1 ศึกษาการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายจากการ Brute Force Attack ด้วยการศึกษากลุ่มข้อมูลเหตุการณ์จาก Honeypot เพื่อนำมาบันทึกในระบบ SIEM จากนั้นทำการวิเคราะห์และสร้างเงื่อนไขการเฝ้าระวัง ป้องกันการโจมตีและแจ้งเตือนภัยคุกคาม ส่วนที่ 2 เป็นการประเมินความเหมาะสมและการยอมรับของการออกแบบ Proposed Zero Trust Security Architecture

ผลวิจัยพบว่า ส่วนที่ 1 กระบวนการป้องกันการโจมตีภัยคุกคาม บนเครื่องคอมพิวเตอร์แม่ข่าย และการแจ้งเตือนแบบเรียลไทม์ ประกอบด้วย 3 ขั้นตอน คือ 1) การรวบรวมข้อมูล Log System 2) การ

วิเคราะห์การโจมตี 3) การสร้างเงื่อนไขการเฝ้าระวัง ป้องกันและการแจ้งเตือน ซึ่งผู้วิจัยพบว่า ประสิทธิภาพจากการป้องกันแบบเรียลไทม์ ด้วยการวิเคราะห์เปรียบเทียบค่าเงื่อนไขกับ Log System มีค่าประสิทธิภาพการป้องกันแบบเรียลไทม์อยู่ในระดับมากที่สุดที่สุด ($\bar{X}= 5.00$) และ ประสิทธิภาพการแจ้งเตือนแบบเรียลไทม์อยู่ในระดับมากที่สุดที่สุด ($\bar{X}= 5.00$) และเมื่อนำระบบ SIEM ให้หน่วยงานต่างๆ ทำการประเมินความพึงพอใจของผู้ใช้งานระบบ SIEM ปรากฏว่าอยู่ในระดับมากที่สุด ($\bar{X}= 4.34$)

ผลการวิจัยใน ส่วนที่ 2 เป็นผลการประเมินความเหมาะสมและการยอมรับของการออกแบบ Proposed Zero Trust Security Architecture เพื่อนำไปปรับใช้กับองค์กร โดยได้นำเสนอต่อผู้ทรงคุณวุฒิ เพื่อทำการประเมินการออกแบบสถาปัตยกรรมดังกล่าว ปรากฏว่าผลการประเมินก็อยู่ในระดับมากที่สุด ($\bar{X}= 4.67$) ด้วยเช่นกัน

THESIS TITLE	DEVELOPING CYBER THREAT PREVENTION AND ALERT SYSTEMS ON THE SERVER USING REAL-TIME THREAT RESPONSE EVENT ANALYSIS TECHNIQUES
KEYWORDS	CYBER THREAT, CYBER THREAT PREVENTION, CYBER THREAT ALERT
STUDENT	MR.KIT SRINGENDEE
ADVISOR	ASSIST.PROF.DR. SURASAK MUNGSING
CO-ADVISOR	PROF.DR. PRASONG PRANEETPOLGRANG
LEVEL OF STUDY	MASTER OF SCIENCE IN INFORMATION TECHNOLOGY
FACULTY	SCHOOL OF INFORMATION TECHNOLOGY SRIPATUM UNIVERSITY
ACADEMIC YEAR	2023

ABSTRACT

This research aims to: 1) analyze cyber threats on enterprise servers, 2) develop a cyber threat protection and alert system using real-time event response analysis techniques, 3) evaluate the effectiveness of the protection and alert system on enterprise servers, and 4) propose a new Zero Trust Security Architecture suitable for organizations. The research is conducted in two parts. The first part involves studying server attacks through Brute Force Attack by collecting event data from a Honeypot, which is then recorded in a Security Information and Event Management (SIEM) system. This data is analyzed to establish monitoring, prevention, and alert conditions for cyber threats. The second part assesses the suitability and acceptance of the proposed Zero Trust Security Architecture by experts.

The research findings indicate that the real-time threat prevention and alert system for enterprise servers consists of three key steps: 1) collecting Log System data, 2) analyzing attacks, and 3) creating monitoring, prevention, and alert conditions. The study shows that the real-time protection

system is highly effective, with performance ratings at the highest level ($\bar{X}= 5.00$). Similarly, the real-time alert system's effectiveness is also rated at the highest level ($\bar{X}= 5.00$). User satisfaction with the SIEM system, as evaluated by various departments, was very high ($\bar{X}= 4.34$)

In the second part of the study, the proposed Zero Trust Security Architecture was evaluated by experts, and the findings indicated that the design is highly effective ($\bar{X}= 4.67$). The results suggest that the developed real-time cyber threat protection and alert system is highly effective for enterprise servers. Additionally, the proposed Zero Trust Security Architecture is well-suited for organizational implementation, demonstrating significant potential for enhancing cyber security in enterprise environments.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จได้ด้วยดี ด้วยความกรุณาจากหลาย ๆ ท่าน หากจะพูดถึงความสำเร็จของวิทยานิพนธ์นี้ ขอขอบคุณถึงความแรงกล้าและความมุ่งมั่นของท่านอาจารย์ที่ปรึกษาผู้เป็นที่เคารพรัก ของกลุ่ม Thesis Pro ได้แก่ ท่าน ศาสตราจารย์ ดร.ประสงค์ ปรานิตพลกรัง ซึ่งเมื่อก่อนเริ่มต้นที่จะมีการตัดสินใจทำวิจัย หรือ สารนิพนธ์ โดยท่านให้หลักการทำงานแบบมีการวางแผนงานตั้งแต่เริ่มการทำวิจัย มีขั้นตอนอย่างไรบ้าง การมองหาแนวคิดตามหลักวิชาการ แล้วแรงบันดาลใจในการตัดสินใจ พลัดดันตัวเองออกจากกรอบแนวความคิดในสิ่งที่เป็นไปได้ ว่าเราได้ เพื่อนำเสนอมุมมองใหม่ให้เกิดสิ่งที่แตกต่าง เพื่อทำมองข้ามสิ่งเหล่านั้นและลงมือทำ จากการศึกษางานวิจัยที่เกี่ยวข้อง เพื่อนำมาปรับใช้ งานวิจัยของผมให้น่าสนใจ และครบถ้วนตามองค์ประกอบต่างๆ ของหลักการ การทำวิจัย และโดยการสรุปผลงานวิจัยในการนำไปปรับใช้ให้เกิดเป็นแนวทางปฏิบัติใหม่ๆ ที่น่าสนใจ แต่ยังคงยึดหลักมาตรฐานสากล หากเกิดประเด็นสอบถามท่านอาจารย์ยังคงสละเวลาส่วนตัวเพื่อช่วยชี้แนะและคำแนะนำ ในสิ่งที่มองข้ามเพื่อครบถ้วนของเนื้อหา ทั้งการตรวจสอบข้อผิดพลาดในงานวิจัย การขัดเกลาเนื้อหาให้ถูกต้องตามหลักการเขียนงานวิจัย และการส่งเสริมให้วิทยานิพนธ์นี้มีความเข้มแข็งและมีคุณภาพตามมาตรฐานที่กำหนดไว้

ขอขอบคุณอีกหนึ่งท่านคือ ผู้ช่วยศาสตราจารย์ ดร.สุรศักดิ์ มั่งสิงห์ ที่ให้คำแนะนำและความเป็นห่วงเป็นใยแก่นักศึกษาทุกครั้งที่ได้มีการประชุม พบปะพูดคุยเสมอมา อีกทั้งความตั้งใจอย่างแรงกล้าและความมุ่งมั่นของทีมงาน Thesis Pro และเพื่อน ๆ SPU M.S.IT 28 ที่ให้กำลังใจมาโดยตลอด

ด้วยการรับรู้และการปลุกดันต่าง ๆ รวมถึงคำแนะนำของคณะกรรมการสอบวิทยานิพนธ์ และผู้ทรงคุณวุฒิทุกท่าน ที่ได้ช่วยแบ่งปันความรู้และแนวทางการศึกษางานวิจัย ถือว่าเป็นประสบการณ์ที่ดีมากที่ได้รับ และเป็นแรงสำคัญที่ช่วยนำไปสู่ความสำเร็จในการดำเนินงานวิจัยอื่น ๆ ต่อไป โดยทุกคำแนะนำที่ได้รับไม่เพียงแต่ช่วยให้การเก็บข้อมูลและการวิเคราะห์มีประสิทธิภาพ แต่ยังเป็นแรงบันดาลใจให้ผมสร้างงานวิจัยที่สมบูรณ์และมีคุณค่าอีกด้วย

งานวิจัยได้รับความครบถ้วนและสมบูรณ์ มากยิ่งขึ้นจากคำแนะนำของคณะกรรมการที่ผู้สอบหัวข้อและสอบป้องกันวิทยานิพนธ์ทั้ง ผู้ช่วยศาสตราจารย์ ดร.ปราณี มณีรัตน์ และ ผู้ช่วยศาสตราจารย์

ดร.พายัพ ศิรินาม ให้คำแนะนำเชิงลึกและการปรับปรุงเนื้อหาบางส่วนให้มีความเข้มข้นและเข้าใจในงานวิจัยได้และสะท้อนถึงความเข้าใจในงานวิจัยมากยิ่งขึ้น

นอกจากนี้ ขอขอบคุณ มหาวิทยาลัยศรีปทุม คณบดี อาจารย์ และเจ้าหน้าที่ของคณะเทคโนโลยีสารสนเทศ ที่ได้ให้การสนับสนุนและเอื้อเฟื้อสิ่งต่าง ๆ เพื่อให้งานวิจัยของผมเป็นไปอย่างราบรื่น รวมถึงความเชื่อมั่นของท่านที่มีต่องานวิจัยของผม ซึ่งเป็นกำลังใจอย่างดียิ่งในการทำงานวิจัยนี้ให้มีคุณค่าและประโยชน์ต่อองค์กร ทั้งนี้การได้รับข้อมูลจากผู้โจมตีเข้ามาทดสอบระบบ ทำให้เกิดการพัฒนา และท่านอาจารย์ทุกท่านที่เป็นคณะกรรมการสอบงานวิจัยนี้ได้ให้การชี้แนะต่าง ๆ เพื่อการปรับปรุงเนื้อหางานวิจัยให้ครบถ้วนในด้านต่าง ๆ และสามารถนำความรู้จากคำแนะนำที่ได้ไปพัฒนาการทำงานของวิจัยต่อไปในอนาคตได้อีกด้วย

ด้วยความพยายามในการทำงานวิจัย ผมหวังว่างานวิจัยฉบับนี้จะเป็นประโยชน์และสามารถประยุกต์ใช้ในองค์กร หรือเพื่อเป็นประโยชน์ในการศึกษาและพัฒนางานวิจัยในอนาคต ด้วยแนวคิดและความเชื่อมั่นที่ได้รับจากคณาจารย์หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ ที่ได้แนะนำและเสนอแนวทางการนำความรู้ไปช่วยเสริมสร้างการใช้เทคโนโลยีเพื่อธุรกิจ

สุดท้าย ขอขอบพระคุณ มหาวิทยาลัยศรีปทุม คณบดี อาจารย์ และเจ้าหน้าที่ทุกท่าน ที่ได้ให้ความเชื่อมั่นและสนับสนุนในการดำเนินงานวิจัยนี้ ความร่วมมือและการสนับสนุนของท่านเป็นปัจจัยสำคัญในการทำให้วิทยานิพนธ์นี้สำเร็จ ขอขอบคุณทุกท่านที่มีส่วนร่วมในการทำให้วิทยานิพนธ์นี้สำเร็จอย่างยิ่งใหญ่ ความร่วมมือและความเชื่อมั่นของทุกท่านเป็นพลังที่สำคัญในการผลักดันให้ก้าวไปสู่ความสำเร็จ จึงหวังว่าผลงานนี้จะมีประโยชน์และคุณค่าต่อองค์กรและชุมชนในที่สุด ขอขอบคุณอย่างสูงสำหรับความมุ่งมั่นและความร่วมมือของทุกท่าน

ด้วยความเคารพและซาบซึ้งใจ

กฤษ ศรีเงินดี

5 สิงหาคม 2567

สารบัญ

	หน้า
บทคัดย่อภาษาไทย.....	I
บทคัดย่อภาษาอังกฤษ.....	II
กิตติกรรมประกาศ.....	III
สารบัญ.....	IV
สารบัญตาราง.....	VII
สารบัญภาพ.....	VIII

บทที่	หน้า
1 บทนำ.....	1
1.1 ความเป็นมาและความสำคัญของปัญหา.....	1
1.2 คำถามการวิจัย.....	4
1.3 วัตถุประสงค์ของการวิจัย.....	5
1.4 สมมติฐานการวิจัย.....	5
1.5 กรอบแนวคิดในการวิจัย.....	5
1.6 ขอบเขตของการวิจัย.....	6
1.7 แผนการในการทำวิจัย.....	6
1.8 ประโยชน์ที่คาดว่าจะได้รับ.....	7
1.9 นิยามศัพท์เฉพาะ.....	7
1.10 สรุป.....	8
2 แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง.....	9
2.1 แนวคิดเกี่ยวกับภัยคุกคามทางไซเบอร์.....	9
2.2 แนวคิดเกี่ยวกับการโจมตีทางไซเบอร์.....	19
2.3 แนวคิดเกี่ยวกับอาชญากรรมทางไซเบอร์.....	23
2.4 แนวคิดและทฤษฎีการกระทำที่เป็นกิจวัตร (Theory of Routine Activity)	29
2.5 หลักการเกี่ยวกับ MITRE ATT&CK Framework	32
2.6 หลักการเกี่ยวกับระบบ Security Information & Event Management (SIEM).....	42
2.7 หลักการวงจรการพัฒนาารบบ (System Development Life Cycle: SDLC)	47
2.8 หลักการเกี่ยวกับ Zero Trust Architecture.....	48

สารบัญ (ต่อ)

บทที่	หน้า
2.9 หลักการเกี่ยวกับ Cybersecurity Mesh Architecture.....	52
2.10 งานวิจัยที่เกี่ยวข้อง.....	56
2.11 สรุป.....	62
3 วิธีดำเนินการวิจัย.....	63
3.1 ขั้นตอนการดำเนินงานวิจัย.....	63
3.2 เครื่องมือใช้ในการวิจัย.....	70
3.3 ออกแบบและพัฒนาการตอบสนองการโจมตีและการแจ้งเตือน.....	80
3.4 ทดสอบการป้องกันการโจมตีและการแจ้งเตือน.....	85
3.5 การประเมินประสิทธิภาพการโจมตีแบบเรียลไทม์และแจ้งเตือน.....	87
3.6 ข้อยกเว้นทางงานวิจัย.....	89
3.7 สรุป.....	90
4 ผลการวิจัย.....	91
4.1 ผลการวิจัยวัตถุประสงค์ข้อที่ 1.....	92
4.2 ผลการวิจัยวัตถุประสงค์ข้อที่ 2.....	99
4.3 ผลการวิจัยวัตถุประสงค์ข้อที่ 3.....	106
4.4 ผลการวิจัยวัตถุประสงค์ข้อที่ 4.....	115
4.5 สรุป.....	133
5 สรุปผลการวิจัยอภิปรายผลและข้อเสนอแนะ.....	135
5.1 สรุปผลการวิจัย.....	135
5.2 อภิปรายผล.....	136
5.3 ปัญหาและอุปสรรคในการทำวิจัย.....	142
5.4 ข้อเสนอแนะ.....	143

สารบัญ (ต่อ)

บรรณานุกรม.....	145
ภาคผนวก ก แบบทดสอบประสิทธิภาพการวิเคราะห์การป้องกันและแจ้งเตือนภัยคุกคาม ทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์ เหตุการณ์ตอบสนองแบบเรียลไทม์.....	150
ภาคผนวก ข คู่มือการใช้งานแอปพลิเคชัน SIEM.....	163
ภาคผนวก ค ใบตอบรับการตีพิมพ์และวารสารที่ได้รับการตีพิมพ์.....	171
ภาคผนวก ง แบบประเมินความเหมาะสมของ Proposed Zero Trust Security Architecture แบบใหม่.....	197
ภาคผนวก จ แบบประเมินความพึงพอใจของผู้ใช้แอปพลิเคชันสำหรับป้องกันและ แจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิค การวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์.....	208
ภาคผนวก ฉ ข้อมูลประวัติผู้ทรงคุณวุฒิ.....	215
ภาคผนวก ช หนังสือที่ออกจากมหาวิทยาลัย.....	220
ภาคผนวก ซ หนังสือรับรองการใช้ประโยชน์.....	227
ประวัติผู้วิจัย.....	237

สารบัญตาราง

ตารางที่	หน้า
1.1 แสดงระยะเวลาในการดำเนินงาน	7
3.1 แสดงระดับและจำนวนคะแนน	87
3.2 แสดงระดับค่าเฉลี่ยอันตรภาคชั้น	88
3.3 ระดับค่าเบี่ยงเบนมาตรฐานการทดสอบ	89
4.1 ผลระยะเวลาการป้องกันแบบเรียลไทม์ เงื่อนไขที่ 100030	108
4.2 ผลระยะเวลาการป้องกันแบบเรียลไทม์ เงื่อนไขที่ 100040	108
4.3 ผลระยะเวลาการแจ้งเตือนแบบเรียลไทม์ เงื่อนไขที่ 100030	108
4.4 ผลระยะเวลาการแจ้งเตือนแบบเรียลไทม์ เงื่อนไขที่ 100040	108
4.5 ข้อมูลเพศของผู้ตอบแบบประเมิน	109
4.6 ข้อมูลอายุของผู้ตอบแบบประเมิน	110
4.7 ข้อมูลระดับการศึกษาของผู้ตอบแบบประเมิน	110
4.8 ข้อมูลประสบการณ์ทำงานของผู้ตอบแบบประเมิน	110
4.9 ข้อมูลของประเภทหน่วยงาน	111
4.10 ข้อมูลการดำเนินงานของหน่วยงาน	111
4.11 ผลการประเมินด้านระบบตรงกับความต้องการของผู้ใช้	112
4.12 ผลการประเมินด้านการทำงานได้ตามฟังก์ชันงานของระบบ	112
4.13 ผลการประเมินด้านความง่ายต่อการใช้งานระบบ	113
4.14 ผลการประเมินด้านประสิทธิภาพการทำงานของระบบ	113
4.15 ผลการประเมินด้านความปลอดภัยของระบบ	114
4.16 ผลร่วมการประเมินความพึงพอใจในแต่ละด้าน	114
4.17 สรุปเปรียบเทียบการกำกับด้านต่างๆ ของ Framework และ Standard	118
4.18 ข้อมูลทั่วไปของผู้ทรงคุณวุฒิ	127
4.19 ผลการประเมินประเด็นสอบถาม	129
4.20 ผลการประเมินระดับความเหมาะสมหรือการยอมรับ	132

สารบัญภาพ

ภาพประกอบที่	หน้า
1.1 รายงานสถิติภัยคุกคาม สกมช. ประจำปี พ.ศ. 2565-2566	1
1.2 รายงานสถิติรูปแบบภัยคุกคาม สกมช. ประจำปี พ.ศ. 2565-2566	2
1.3 แสดง Understanding The SIEM Architecture	3
1.4 แสดง Basic Slack Architecture	3
1.5 กรอบแนวคิดในการวิจัย	6
2.1 แสดงประเภทภัยคุกคามทางไซเบอร์ที่พบบ่อย	10
2.2 แสดงประเภทภัยคุกคามทางไซเบอร์ที่พบบ่อย	11
2.3 แรนซัมแวร์ ฟุ่งเป้า ภาคธุรกิจ เพิ่ม 363%	12
2.4 แสดงประเภทภัยคุกคาม Phishing Mail	13
2.5 แสดงประเภทภัยคุกคาม SQL Injection Attacks	14
2.6 แสดงรูปแบบ Brute Force Attack	15
2.7 แสดงประเภทภัยคุกคาม Cross-Site Scripting (XSS)	16
2.8 แสดงประเภทภัยคุกคาม Distributed Denial-of-Service (DDos)	17
2.9 แสดงประเภทภัยคุกคาม Man-in-the-Middle Attacks	18
2.10 แสดง SMBประสบเหตุการณ์ทางไซเบอร์	20
2.11 แสดงสถิติคดีอาชญากรรมทางเทคโนโลยี	24
2.12 แสดงแบ่งประเภทของอาชญากรรมทางไซเบอร์	25
2.13 แสดงสถิติ Cyber Bullying ระดับชั้น ม.1-ม.3 ปี 2560	26
2.14 แสดงสถิติ Hate Crime 20 รัฐใหญ่ ประเทศสหรัฐอเมริกา 2015	27
2.15 แสดง Crime Triangle Theory	28
2.16 แสดง Routine Activities Theory	29
2.17 แสดงแนวโน้มอาชญากรรมระหว่างประเทศและอาชญากรรมที่เกิดขึ้นใหม่ COVID-19	31
2.18 แสดง Evolution of MITRE ATT&CK Timeline	33
2.19 แสดง ATT&CK Objects are modelled	34
2.20 แสดง MITRE ATT&CK TACTICS: ENTERPRISE	35
2.21 แสดง Log point Top 10 Critical MITRE ATT&CK Techniques	40
2.22 แสดง การทำงานของ SEIMและความสามารถที่โดดเด่น	43
2.23 แสดง กระบวนการทำงานของ SIEM มีอะไรบ้าง	45

สารบัญภาพ (ต่อ)

ภาพประกอบที่	หน้า
2.24 แสดง How Security Information and Event Management (SIEM) Works	46
2.25 แสดง History Software development life cycle	47
2.26 แสดง Seven Phases of Software Development Life Cycle	48
2.27 แสดง Zero Trust Maturity Model Pillars	49
2.28 แสดง Network Castle and Moat Model	50
2.29 แสดง Network Zero Trust Model	51
2.30 แสดง Cybersecurity Mesh Architecture Concept	53
3.1 แสดง การจัดเก็บ Log ระบบ SIEM System	64
3.2 แสดงเครื่องคอมพิวเตอร์แม่ข่ายใช้เป็น Honeypot	65
3.3 แสดงสถานะการทำงานของ Agent บน Honeypot	65
3.4 แสดงการส่งค่า Log ระหว่าง Agent กับ SIEM	66
3.5 แสดง แสดง SIEM Flow System	67
3.6 แสดงบันทึก Log System จาก Agent	67
3.7 แสดงค่าเปรียบเทียบของ MITRE ATT&CK Framework	68
3.8 แสดง การเชื่อมต่อระหว่างระบบของ SIEM	69
3.9 แสดงเงื่อนไขการป้องกัน Brute Force แบบเรียลไทม์	69
3.10 แสดง Basic Wazuh Workflow	71
3.11 แสดง Log System ที่ทำการเก็บบันทึก	72
3.12 แสดงตัวอย่างการจัดเก็บ Log System CentOS7	72
3.13 แสดง แดชบอร์ดอินเตอร์เฟซผู้ใช้งาน	73
3.14 แสดง Data Flow Message	74
3.15 แสดง CentOS Version	75
3.16 แสดง รายละเอียด CentOS Version	76
3.17 แสดง Webmin Configuration	77
3.18 แสดง Basic architecture of an Amazon EC2	78
3.19 แสดง Amazon EC2 Service	78
3.20 แสดง Kali Linux Timeline	79
3.21 แสดง เครื่องมือที่ใช้โจมตี Password	79

สารบัญภาพ (ต่อ)

ภาพประกอบที่	หน้า
3.22 แสดง System Design	80
3.23 แสดง Use Case Diagram แพลตฟอร์มจัดการ SIEM	81
3.24 แสดงไฟล์กำหนดกฎใน SIEM	82
3.25 แสดง System Auto Block SSH	82
3.26 แสดง การตั้งเงื่อนไขการป้องกันแบบเรียลไทม์	83
3.27 แสดง การตั้งเงื่อนไขการส่งข้อความทาง Slack	83
3.28 แสดง การกำหนดพารามิเตอร์ส่งข้อความทาง Slack	84
3.29 แสดง ข้อความการแจ้งเตือนทาง Slack	84
3.30 แสดงเครื่องมือ Hydra	85
3.31 แสดงเครื่องมือ Medusa	86
3.32 แสดงเครื่องมือ Ncrack	86
4.1 แสดงขั้นตอนการทำงานของระบบ SIEM	92
4.2 แสดงการกำหนดเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย Honeypot	93
4.3 แสดงจำนวนเหตุการณ์บนเครื่องคอมพิวเตอร์แม่ข่าย Honeypot	94
4.4 แสดงจำนวน Rule.id 5503, 5760 สุ่มรหัสผ่านแบบผู้ใช้เป็น Root	94
4.5 แสดงรายละเอียด Rule.id 5760 สุ่มรหัสผ่านแบบผู้ใช้เป็น Root	95
4.6 แสดงจำนวน Rule.id 5710 สุ่มรหัสผ่านแบบผู้ใช้ไม่ใช่ Root	95
4.7 แสดงรายละเอียด Rule.id 5710 สุ่มรหัสผ่านแบบไม่ใช่ Root	96
4.8 แสดงการเข้ามาค้นหาพอร์ตเครื่องคอมพิวเตอร์แม่ข่าย	96
4.9 แสดงรายละเอียดการค้นหาการบริการเครื่องคอมพิวเตอร์แม่ข่าย	97
4.10 แสดงเทคนิคเปรียบเทียบกับ MITRE ATT&CK	97
4.11 แสดงรายละเอียด rule.id และ rule.mitre.id	98
4.12 แสดงรายละเอียดเข้าเครื่องคอมพิวเตอร์แม่ข่ายอย่างสมบูรณ์	99
4.13 แสดงรายละเอียดเงื่อนไขพฤติกรรมการโจมตีเครื่องคอมพิวเตอร์แม่ข่าย	99
4.14 แสดงทดสอบเงื่อนไข rule.id = 100030	100
4.15 แสดงทดสอบเงื่อนไข rule.id = 100040	101
4.16 แสดงเงื่อนไขส่งชุดคำสั่งไปเครื่องคอมพิวเตอร์แม่ข่าย สำหรับระงับการเข้าถึง	101

สารบัญภาพ (ต่อ)

ภาพประกอบที่	หน้า
4.17 แสดงเงื่อนไขส่งชุดคำสั่งการป้องกันไปยังเครื่องคอมพิวเตอร์แม่ข่าย ผ่าน Agent	102
4.18 แสดงเงื่อนไขส่งชุดคำสั่งการแจ้งเตือนไปยัง Slack ผ่าน API	102
4.19 แสดงเงื่อนไขส่งชุดคำสั่งการแจ้งเตือนไปยัง Slack ผ่าน API	103
4.20 แสดงเงื่อนไขภาษาไพทอนเป็นรูปแบบ Json ไปยัง Slack ผ่าน API	103
4.21 แสดงข้อความการแจ้งเตือน Slack ผ่าน Application	104
4.22 แสดงค่าการโจมตีตรงเงื่อนไขการป้องกัน Brute-Force SSH	105
4.23 แสดงการป้องกัน Brute-Force SSH แบบเรียลไทม์	105
4.24 แสดงเครื่องมือที่ใช้ในการทดสอบ Brute-Force SSH	107
4.25 Proposed Zero Trust Security Architecture	121
5.1 ระดับความพร้อมของความรู้และเทคโนโลยีทางด้านเทคโนโลยี	138
5.2 ระดับความพร้อมของความรู้และเทคโนโลยีทางด้านสังคม	139
ก. 1 เงื่อนไขที่100030ทดสอบครั้งที่ 1	151
ก. 2 เงื่อนไขที่100030ทดสอบครั้งที่ 2	152
ก. 3 เงื่อนไขที่100030ทดสอบครั้งที่ 3	152
ก. 4 เงื่อนไขที่100030ทดสอบครั้งที่ 4	153
ก. 5 เงื่อนไขที่100030ทดสอบครั้งที่ 5	153
ก. 6 แจ้งเตือน100030ทดสอบครั้งที่ 1	154
ก. 7 แจ้งเตือน100030ทดสอบครั้งที่ 2	154
ก. 8 แจ้งเตือน100030ทดสอบครั้งที่ 3	155
ก. 9 แจ้งเตือน100030ทดสอบครั้งที่ 4	155
ก.10 แจ้งเตือน100030ทดสอบครั้งที่ 5	156
ก.11 เงื่อนไขที่100040ทดสอบครั้งที่ 1	157
ก.12 เงื่อนไขที่100040ทดสอบครั้งที่ 2	157
ก.13 เงื่อนไขที่100040ทดสอบครั้งที่ 3	158
ก.14 เงื่อนไขที่100040ทดสอบครั้งที่ 4	158
ก.15 เงื่อนไขที่100040ทดสอบครั้งที่ 5	159

สารบัญภาพ (ต่อ)

ภาพประกอบที่	หน้า
ก.16 แจ๊งเตือน100040ทดสอบครั้งที่ 1	160
ก.17 แจ๊งเตือน100040ทดสอบครั้งที่ 2	160
ก.18 แจ๊งเตือน100040ทดสอบครั้งที่ 3	161
ก.19 แจ๊งเตือน100040ทดสอบครั้งที่ 4	161
ก.20 แจ๊งเตือน100040ทดสอบครั้งที่ 5	162
ข. 1 หน้าล็อกอินเข้าสู่ระบบ SIEM	164
ข. 2 แสดงหน้าจอ Dashboard ของข้อมูลระบบ SIEM	164
ข. 3 แสดงค่าสถานะของ Agent ที่ติดตั้ง	165
ข. 4 แสดงรายละเอียดของเครื่องคอมพิวเตอร์แม่ข่าย ที่ Agent ที่ทำงานอยู่	165
ข. 5 แสดงในส่วนการวิเคราะห์เหตุการณ์ที่ตรวจพบเครื่องคอมพิวเตอร์แม่ข่าย	166
ข. 6 แสดงค่าเปรียบเทียบกับ MITRE, PCI DSS, GDPR, NIST 800-53	166
ข. 7 แสดงรายละเอียดเหตุการณ์ที่เกิดขึ้นในภัยคุกคามที่เข้าเครื่องคอมพิวเตอร์แม่ข่าย	167
ข. 8 แสดง Show Dates เพื่อระบบช่วงเวลาที่ต้อง	167
ข. 9 แสดง Show Dates เพื่อระบบช่วงเวลาที่ต้อง	168
ข.10 แสดง Search และกำหนดช่วงเวลาที่ต้องการค้นหา	168
ข.11 แสดงค่าการค้นหาที่กำหนดไว้	169
ข.12 แสดงหน้า Reporting เพื่อดาวน์โหลดไฟล์รายงาน	169
ข.13 แสดงตัวอย่างรายงานที่สร้างจากระบบ SIEM	170
ข.14 แสดงตัวอย่างค่าการวิเคราะห์อย่างรายงานระบบ SIEM	170

บทที่ 1

บทนำ

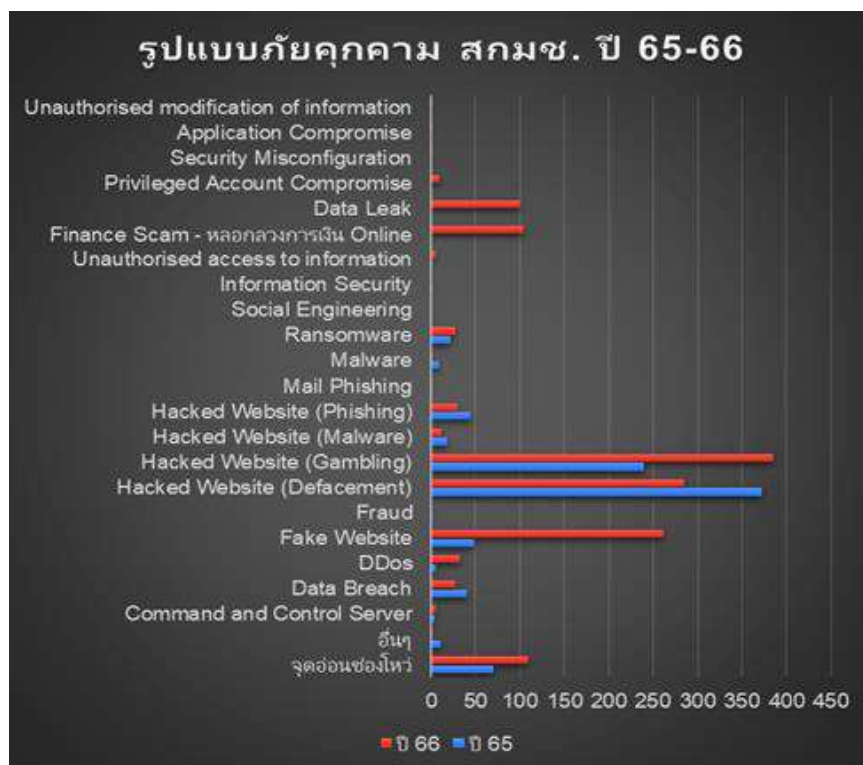
1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเราคงหลีกเลี่ยงไม่ได้ว่าการเข้าถึงใช้งานอินเทอร์เน็ต มีหลากหลายมิติที่สามารถพบเจอได้ในทุกวันนี้ ซึ่งผลมาจากเหตุการณ์ โควิด-19 เป็นกระตุ้นให้การใช้งานระบบบริการต่าง ๆ ผ่านอินเทอร์เน็ตมากขึ้นตามลำดับ ทั้งในส่วนภาครัฐหรือ เอกชนและโดยเฉพาะ SME ที่มีความเสี่ยงและตกเป็นเหยื่อทางไซเบอร์จำนวนมากแต่ไม่มีงบประมาณดูแล ก็มักจะทำให้ผู้ที่ไม่หวังดีต้องการแสวงหาผลประโยชน์จากข้อมูลที่ผู้ใช้งานในระบบอินเทอร์เน็ต และต้องการเข้าถึงระบบแม่ข่ายเพื่อทำให้เกิดความเสียหายต่อการให้บริการ ไม่ว่าทางด้านข้อมูลหรือความน่าเชื่อถือของผู้ให้บริการ

ไม่ว่าด้วยเหตุผลใดเหตุผลหนึ่ง ก็ล้วนแต่สร้างความเสียหายต่อผู้ให้บริการและผู้ใช้บริการต่อระบบการให้บริการนั้น ๆ ซึ่งจากรายงานภัยคุกคามทางไซเบอร์ ประจำปี 2565 ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ดังภาพประกอบที่ 1.1 และ 1.2



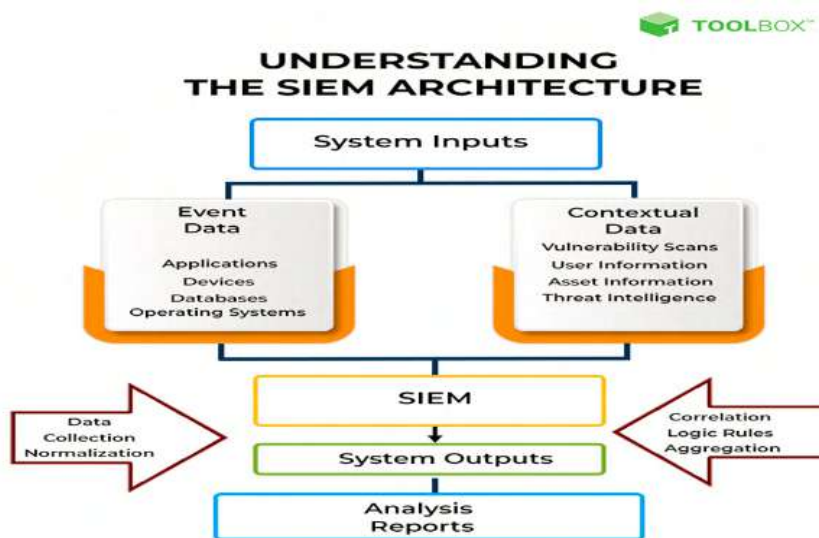
ภาพประกอบที่ 1.1 รายงานสถิติภัยคุกคาม สกมช. ประจำปี พ.ศ. 2565-2566



ภาพประกอบที่ 1.2 รายงานสถิติรูปแบบภัยคุกคาม สกมช. ประจำปี พ.ศ. 2565-2566

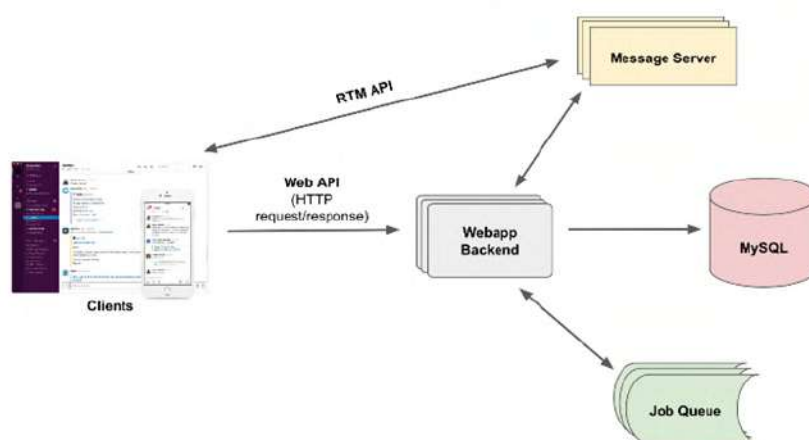
รายงานตั้งแต่เดือนมกราคมถึงธันวาคม มีจำนวน 835 รายการ ซึ่งหากเปรียบเทียบกับ ปี 2566 ระหว่าง มกราคมถึงสิงหาคม ซึ่งมีจำนวน 1,789 รายการ สะท้อนให้เห็นว่าการภัยคุกคามทางไซเบอร์มีแนวโน้มเพิ่มมากขึ้น เมื่อเปรียบเทียบช่วงเวลาเดียว ตั้งแต่มกราคมถึงเดือนสิงหาคม ของปี 2565 พบว่ามีจำนวนเพิ่มขึ้นเป็นร้อยละ 214.2%

Security Information and Event Management (SIEM) คือ โซลูชันการรักษาความมั่นคงปลอดภัยที่ช่วยองค์กรตรวจหา วิเคราะห์ และตอบสนองต่อภัยคุกคามทางไซเบอร์ก่อนที่จะเป็นอันตรายต่อธุรกิจ และการจัดการเหตุการณ์รักษาความปลอดภัย บริษัท Gartner เป็นผู้กำหนดคำว่า SIEM สำหรับการผสมผสานระหว่างเทคโนโลยี SIM และ SEM ในปี 2548 (IBM, 2023) ซึ่งเทคโนโลยี SIEM จะรวบรวมข้อมูลเหตุการณ์จากแหล่งต่าง ๆ ระบุกิจกรรมด้วยการวิเคราะห์แบบเรียลไทม์ ดังภาพประกอบที่ 1.3



ภาพประกอบที่ 1.3 แสดง Understanding The SIEM Architecture
ที่มา Spiceworks.com, 2022

Slack ย่อมาจาก Searchable Log of All Conversation and Knowledge ถูกเปิดตัวขึ้นมาในปี 2013 (Lumb, 2014) ด้วยสถาปัตยกรรมดังภาพประกอบที่ 1.4



ภาพประกอบที่ 1.4 แสดง Basic Slack Architecture
ที่มา <https://slack.engineering> , 2019

จากในรูปที่ 1.4 เป็นแพลตฟอร์มที่ทำให้เราสามารถทำการสื่อสารกับทีมทั้งหมดได้ภายในทีเดียว และแพลตฟอร์มมีหลากหลายความสามารถ เช่น การโทรหากัน การส่งข้อความ หรือการแชร์ไฟล์ เอกสารต่าง ๆ ซึ่งมีอยู่ใน Slack

ปัจจุบันคอมพิวเตอร์มีประสิทธิภาพในการประมวลผลสูง ซึ่งสอดคล้องกับกฎของมัวร์ (Moore's law) (<https://web.ku.ac.th> (University, 1999) ที่ว่า “จำนวนทรานซิสเตอร์บนวงจรรวมจะเพิ่มขึ้นสองเท่าทุก 2 ปี” นั่นหมายความว่า การประมวลผลของคอมพิวเตอร์มีจำนวนมากขึ้น และส่งผลทำให้ประสิทธิภาพในการประมวลผลสูงขึ้นไปด้วย ด้วยความก้าวหน้าทางเทคโนโลยียังมีกลุ่มบุคคลที่ต้องการอาศัยความเร็วในการประมวลผลของคอมพิวเตอร์เพื่อให้เข้าถึงรหัสผ่านแบบสุ่มได้เร็วยิ่งขึ้น

เมื่อมีผู้ไม่หวังดีสามารถเข้าระบบแม้จะขาดจากการได้รหัสผ่าน การสามารถควบคุมเครื่องคอมพิวเตอร์แม้จะได้อย่างสมบูรณ์ ซึ่งเป็นการยากจะเข้าไปควบคุมหรือกู้คืนกลับมาสู่สภาพปกติก่อนเกิดเหตุการณ์ได้ จากแนวโน้มที่ได้กล่าวมาในข้างต้นจึงเห็นว่า เราต้องมีการปรับตัวใช้ระบบเทคโนโลยีที่มีเทคนิคเพิ่มมากขึ้นมาช่วยในการป้องกันและตอบสนองภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพและสอดคล้องกับการให้บริการระบบสารสนเทศได้อย่างต่อเนื่อง อีกทั้งเพิ่มความมั่นใจให้ผู้ให้บริการระบบสามารถมีความปลอดภัยอยู่เสมอ ผู้วิจัยจึงเล็งเห็นว่าสามารถนำการทำงานของระบบ SIEM เข้ามาช่วยในการตอบสนองเหตุการณ์และลดภัยคุกคามแบบเรียลไทม์ได้ไม่น้อยเพียงใด

1.2 คำถามการวิจัย

เมื่อได้ศึกษาถึงแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับการภัยคุกคามทางไซเบอร์ ที่มาจากการบันทึกเหตุการณ์ และวิเคราะห์เหตุการณ์จาก Log Systems ของเครื่องคอมพิวเตอร์แม่ข่ายรวมทั้งการสุ่มรหัสผ่าน และการแจ้งเตือนจนนำไปสู่ข้อสังเกต และข้อคำถามในการวิจัย ดังนี้

1. ภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายในองค์กร เป็นอย่างไร
2. ระบบป้องกัน และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย โดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ ควรเป็นอย่างไร
3. การประเมินประสิทธิภาพของระบบป้องกัน และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย สามารถทำได้อย่างไร
4. แนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ใหม่ที่เหมาะสมกับองค์กร ภายใต้ฐานความคิดที่ไม่ไว้ว่างใจใคร หากแต่ต้องตรวจสอบอยู่เสมอ ควรเป็นอย่างไร

1.3 วัตถุประสงค์ของการวิจัย

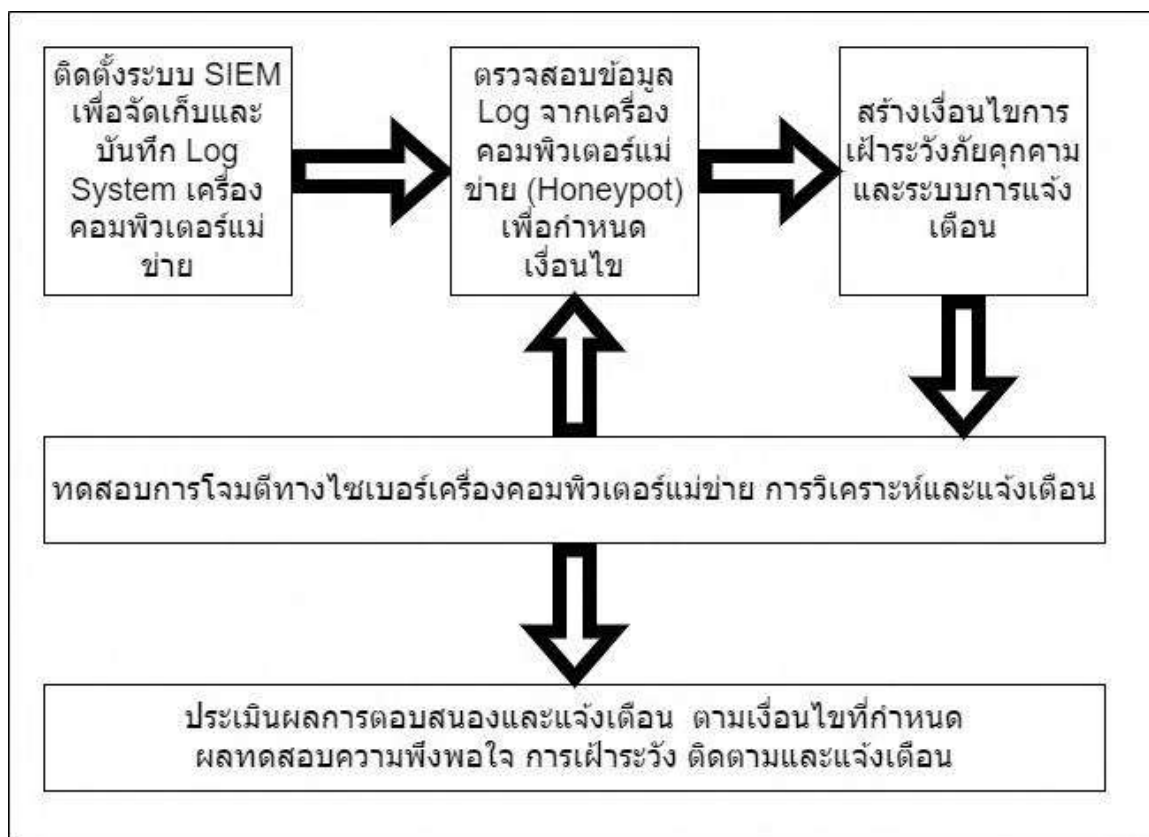
1. เพื่อทำการวิเคราะห์ภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายในองค์กร
2. พัฒนาระบบป้องกัน และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์
3. เพื่อทำการประเมินประสิทธิภาพของระบบป้องกัน และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย
4. นำเสนอแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ใหม่ที่เหมาะสมกับองค์กร ภายใต้งานความคิดที่ไม่ไว้วางใจใคร หากแต่ต้องตรวจสอบอยู่เสมอ

1.4 สมมติฐานการวิจัย

1. ภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายในองค์กร มีค่าความร้ายแรงอยู่ในระดับมาก
2. ระบบป้องกัน และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย โดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ มีประสิทธิภาพอยู่ในระดับมาก
3. ระบบป้องกัน และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย โดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ มีความเหมาะสม และยอมรับอยู่ในระดับมาก
4. แนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ใหม่ที่เหมาะสมกับองค์กร ภายใต้งานความคิดที่ไม่ไว้วางใจใคร หากแต่ต้องตรวจสอบอยู่เสมอ นั้น มีความเหมาะสม เป็นไปได้ และการยอมรับอยู่ในระดับมาก

1.5 กรอบแนวคิดในการวิจัย

การติดตั้งระบบ SIEM บนระบบแม่ข่าย และเครื่องคอมพิวเตอร์แม่ข่ายที่ถูกติดตั้งโปรแกรมเฝ้าระวังผ่านการสอบทาน System Log เพื่อตรวจจับการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการใช้งานผ่านระบบอินเทอร์เน็ต เมื่อระบบ SIEM มีการตรวจจับสิ่งผิดปกติที่เป็นไปตามเงื่อนไขที่กำหนดโดยผู้ดูแลระบบ ระบบ SIEM จะดำเนินการสั่งการให้เครื่องคอมพิวเตอร์แม่ข่ายที่อยู่ในการดูแลของระบบ SIEM สั่งการผ่าน API ไปที่เครื่องคอมพิวเตอร์แม่ข่ายที่มีการติดตั้งโปรแกรมสั่งการ และสอบทาน Log ให้กระทำการตอบสนองทันที ตรงตามเงื่อนไข เพื่อระงับการโจมตีระบบแม่ข่าย ได้ดังภาพประกอบที่ 1.5



ภาพประกอบที่ 1.5 กรอบแนวคิดในการวิจัย

1.6 ขอบเขตของการวิจัย

1. พัฒนาระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์
2. เพื่อทำการประเมินประสิทธิภาพของระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย
3. วิสาหกิจขนาดกลาง และขนาดย่อม ธุรกิจ SME (Small and Medium Enterprises) ด้านบริการเทคโนโลยีสารสนเทศ

1.7 แผนการในการทำวิจัย

การดำเนินงานวิจัยระยะเวลารวมทั้งสิ้น 3 ภาคการศึกษา ตั้งแต่เดือน สิงหาคม พ.ศ. 2566 ถึงเดือน สิงหาคม พ.ศ. 2567 รายละเอียดดังตารางที่ 1.1

ตารางที่ 1.1 แสดงระยะเวลาในการดำเนินงาน

ขั้นตอนการดำเนินงาน	ระยะเวลาในการดำเนินงาน ปีการศึกษา 2566											
	ปี พ.ศ.2566					ปี พ.ศ.2567						
	ก.ย.	ค.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.
1. ศึกษาปัญหาและข้อมูลที่เกี่ยวข้อง												
2. รวบรวมข้อมูลจากเอกสาร และ งานวิจัยที่เกี่ยวข้อง												
3. รวบรวมความต้องการวิเคราะห์และออกแบบระบบ												
4. พัฒนาระบบและทำการทดสอบตัวระบบ												
5. สรุปผลการวิจัยพร้อมประเมินประสิทธิภาพและข้อเสนอแนะ												
6. เรียบเรียงและปรับปรุงงานวิจัย												
7. เสนอผลงานและจัดทำเอกสารงานวิจัย												

1.8 ประโยชน์ที่คาดว่าจะได้รับ

1. ทำให้ค้นพบวิธีการพัฒนาความสามารถการใช้งาน SIEM มาปรับใช้การตอบสนองการโจมตีแบบเรียลไทม์ และนำไปปรับใช้ป้องกันโจมตีทางไซเบอร์ ซึ่งเพิ่มประสิทธิภาพการป้องกันระบบแม้ช่วยได้อย่างมีประสิทธิภาพมากขึ้น
2. เป็นการทำ Open Secure ที่เผยแพร่ความรู้ในการให้คำปรึกษาแก่องค์กร รวมทั้งแนวทางการแก้ปัญหาทางไซเบอร์ให้แก่บุคคลทั่วไป โดยเฉพาะ SME ที่มีความเสี่ยงและตกเป็นเหยื่อทางไซเบอร์จำนวนมากแต่ไม่มีงบประมาณนำไปปรับใช้ได้
3. การนำเสนอกรอบแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมสำหรับ SME

1.9 นิยามศัพท์เฉพาะ

1. โซลูชันการรักษาความปลอดภัยที่ช่วยของค์กรตรวจหา วิเคราะห์ และตอบสนองต่อภัยคุกคามด้านความปลอดภัย (SIEM) หมายถึง แนวทางการรักษาความปลอดภัยที่ช่วยของค์กรตรวจหา วิเคราะห์ และตอบสนองต่อภัยคุกคามด้านความปลอดภัยก่อนที่จะเป็นอันตรายต่อการดำเนินธุรกิจรวมการจัดการข้อมูลการรักษาความปลอดภัย (SIM) และการจัดการเหตุการณ์การรักษาความปลอดภัย (SEM)

ให้เป็นระบบการจัดการการรักษาความปลอดภัยเพียงระบบเดียว ซึ่งเทคโนโลยี SIEM จะรวบรวมข้อมูลบันทึกเหตุการณ์จากแหล่งต่างๆ ระบุกิจกรรมที่เบี่ยงเบนจากบรรทัดฐานด้วยการวิเคราะห์แบบเรียลไทม์ (Security information and event management, 2021)

2. ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) หมายถึง ภาวะพ้นจากภัยคุกคามที่มีต่อโครงข่ายระบบคอมพิวเตอร์ ซอฟต์แวร์ และข้อมูล เพื่อรักษาซึ่งดำรงไว้สำคัญทั้ง 3 ประการ คือ ความลับ ความถูกต้อง และความพร้อมใช้งาน จากที่ได้กล่าวมา หากจะเกิดขึ้นได้ต้องเกี่ยวข้องกับบุคลากร ในขั้นตอนการทำงาน และเครื่องมือที่ถูกต้อง (ราชบัณฑิตยสถานคอมพิวเตอร์ และเทคโนโลยีสารสนเทศ, 2558)

3. อาชญากรรมไซเบอร์ (Cyber Crime) หมายถึง การกระทำความผิดกฎหมายโดยใช้คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เป็นเครื่องมือ เช่น ทำลาย เปลี่ยนแปลง หรือขโมยข้อมูล รวมถึง การทำให้การทำงานของระบบคอมพิวเตอร์หรือระบบเครือข่าย ถูกกระับ ชะลอ ชัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ (สำนักงานราชบัณฑิตยสภา, 2562)

4. การโจมตีทางไซเบอร์ (Cyberattack) หมายถึง การกระทำที่มุ่งร้ายหรือจงใจ โดยมีวัตถุประสงค์เพื่อขัดขวางหรือทำให้การทำงานของระบบสารสนเทศ หรือข้อมูลในระบบสารสนเทศไม่สามารถใช้งานได้ (Chaloemchatwanit, 2021)

5. ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายถึง การกระทำหรือการดำเนินการใด ๆ ที่เป็นอันตรายโดยมี ผ่านการใช้ระบบสารสนเทศหรือเครือข่าย จุดประสงค์มุ่งหมายเพื่อสร้างความเสียหายหรือขโมยข้อมูลจากองค์กรที่ทำให้เกิดการหยุดชะงักของวงจรดิจิทัล รวมถึงทางกายภาพ อาชญากรรมหรือส่วนตัวในการทำลายหรือเข้าถึงข้อมูลที่เป็นความลับ

6. ซีเคียวเชลล์ (Secure Shell) หมายถึง SSH Network Protocol สำหรับการแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์เครือข่ายที่ใช้ Linux หรือ Unix ผ่านช่องทางที่มีความปลอดภัย (Secure Channel) ออกแบบมาเพื่อให้คอมพิวเตอร์เครื่องหนึ่ง (SSH Client) สามารถเข้าถึงหรือควบคุมคอมพิวเตอร์อีกเครื่องหนึ่ง (SSH Server) แบบระยะไกลได้ผ่านอินเทอร์เน็ต

1.10 สรุป

งานวิจัยที่วางกรอบการวิจัยไว้เพื่อมุ่งหวังให้เกิดการพัฒนาการป้องกันภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายแบบเรียลไทม์และเพื่อเสนอการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมสำหรับ SME โดยการพัฒนาความสามารถการใช้งาน SIEM มาปรับใช้การตอบสนองการโจมตีเพิ่มประสิทธิภาพการป้องกันระบบแม่ข่ายได้อย่างมีประสิทธิภาพมากขึ้น

บทที่ 2

แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

การศึกษาและวิจัยในครั้งนี้เป็น เรื่องการพัฒนาการใช้ SIEM ในการบันทึกเหตุการณ์ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายเพื่อจัดเก็บ และจำแนกเหตุการณ์ต่างเปรียบเทียบกับเงื่อนไขที่ระบุไว้ก่อนหน้านี้ เพื่อป้องกันการโจมตีแบบ SSH Brute Force โดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ และแจ้งเตือนผ่านแพลตฟอร์ม Slack ได้อย่างถูกต้อง และทันเหตุการณ์ โดยให้ผู้ดูแลระบบสามารถทราบถึงการป้องกันเครื่องคอมพิวเตอร์แม่ข่ายได้ตลอดเวลา และยังเป็นการตรวจสอบการตอบสนองให้เข้าใจเรื่องการป้องกัน หรือปรับการเข้าถึงระบบแม่ข่าย ครั้งนี้ได้ทำการศึกษาแนวคิด ทฤษฎี เอกสารต่าง ๆ และผลงานวิจัยที่เกี่ยวข้องเพื่อเป็นแนวทางในการวิจัย ดังนี้

- 2.1 แนวคิดเกี่ยวกับภัยคุกคามทางไซเบอร์
- 2.2 แนวคิดเกี่ยวกับการโจมตีทางไซเบอร์
- 2.3 แนวคิดเกี่ยวกับอาชญากรรมทางไซเบอร์
- 2.4 แนวคิดและทฤษฎีการกระทำที่เป็นกิจวัตรประจำวัน (Theory of Routine Activity)
- 2.5 หลักการเกี่ยวกับ MITRE ATT&CK Framework
- 2.6 หลักการเกี่ยวกับระบบ Security Information & Event Management (SIEM)
- 2.7 หลักการวงจรการพัฒนาาระบบ (System Development Life Cycle: SDLC)
- 2.8 หลักการเกี่ยวกับ Zero Trust Architecture
- 2.9 หลักการเกี่ยวกับ Cybersecurity Mesh Architecture
- 2.10 งานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดเกี่ยวกับภัยคุกคามทางไซเบอร์

ปัจจุบันความมั่นคงปลอดภัยภัยคุกคามทางไซเบอร์ที่กระทบต่อความเชื่อมั่น และการให้บริการต่าง ๆ ผ่านอินเทอร์เน็ตมีความสำคัญเป็นลำดับต้น ๆ เมื่อหากมีการให้บริการแก่บุคคลภายนอก หรือภายใน แต่ยังคงอาศัยการเข้าการให้บริการสารสนเทศนั้น ก็ย่อมมีความเสี่ยงต่อภัยคุกคามที่อาจจะเกิดได้

ทุกเมื่อ ซึ่งเป็นเรื่องที่ทำให้ความเข้าใจ และแนวทางการคุกคามหรือโจมตีเพื่อนำปรับใช้หรือป้องกันระบบ ให้มีความมั่นคงมากขึ้น

ภัยคุกคาม (Threat) คือ บุคคล สิ่งของหรือเหตุการณ์ใดๆก็ตามที่มุ่งร้ายหรือเป็นสาเหตุของภัยอันตรายต่างๆที่อาจจะเกิดขึ้นกับระบบคอมพิวเตอร์ ในรูปแบบของการทำร้าย เปิดเผย แก้ไขข้อมูล และรวมถึงการทำให้ระบบไม่สามารถให้บริการแก่ผู้ใช้งานได้โดยภัยคุกคามอาจจะเกิดขึ้นโดยอุบัติเหตุหรือเกิดขึ้นโดยเจตนาของผู้ที่ประสงค์ร้ายต่อระบบ โดยการโจมตีอาจจะเป็นการกระทำโดยพยายามที่จะข้ามผ่านระบบป้องกัน (Bypass) หรือกระบวนการควบคุมความมั่นคงปลอดภัยของระบบคอมพิวเตอร์

ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายความว่า การที่มีภัยคุกคามหรือความเสี่ยงในด้านความมั่นคงปลอดภัยทางไซเบอร์ หรือสถานการณ์ทำให้เกิดความเสียหายหรือส่งผลกระทบต่อระบบคอมพิวเตอร์ ข้อมูล หรือระบบคอมพิวเตอร์โดยใช้เทคโนโลยีสารสนเทศ (IT) หรืออุปกรณ์คอมพิวเตอร์ต่าง ๆ การความเสี่ยงทางไซเบอร์อาจมีหลายรูปแบบตาม ดังภาพประกอบที่ 2.1



ภาพประกอบที่ 2.1 แสดงประเภทภัยคุกคามทางไซเบอร์ที่พบบ่อย

ที่มา : Cyberelite, 2565

ไซเบอร์ (Cyber) หมายความว่า ข้อมูลและการสื่อสารข้อมูลที่เกิดจากการให้บริการหรือประยุกต์ใช้ผ่านทางเครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายการสื่อสารใดๆ ที่มีความคล้ายคลึงกันอีกด้วย ที่เชื่อมต่อกันเป็นการทั่วไป

2.1.1 มัลแวร์

มัลแวร์ (Malware) หมายถึง นั้นย่อมาจาก Malicious และ ซอฟต์แวร์หมายถึง โปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมาเพื่อทำอันตรายกับข้อมูลในระบบ เช่น ทำให้เครื่องคอมพิวเตอร์ทำงานผิดปกติ ขโมยหรือทำลายข้อมูลโดยมีมัลแวร์ที่ตรวจพบบ่อย ดังภาพประกอบที่ 2.2



ภาพประกอบที่ 2.2 แสดงประเภทภัยคุกคามทางไซเบอร์ที่พบบ่อย
ที่มา : Facebook ETDA, 2564

ประเภทของมัลแวร์ เช่น

ไวรัส (Viruses) ไวรัสเป็นโปรแกรมคอมพิวเตอร์ที่สามารถคัดลอกสำเนาตัวเองและสามารถแพร่กระจายไปยังไฟล์อื่น ๆ บนคอมพิวเตอร์ของผู้ใช้งาน โดยเดิมโค้ดที่อันตรายลงในไฟล์เหล่านั้น โดยที่ผู้ใช้งานไฟล์หรือส่งไฟล์นั้นให้กับผู้อื่น สามารถทำให้เครื่องคอมพิวเตอร์ผู้นั้นติดไวรัสได้เช่นกัน

โทรจัน (Trojans) โทรจันเป็นมัลแวร์ที่ถูกสร้างขึ้นมาเพื่อหลอกเราว่า มันเป็นโปรแกรมปกติทั่วไปที่สามารถใช้งานได้ปกติ และดูไม่มีพิษภัย เมื่อผู้ใช้งานหลงเชื่อแล้วนำไปติดตั้งบนคอมพิวเตอร์ของผู้ใช้งานเรียบร้อยแล้วจะสามารถส่งข้อมูลหรือเข้าถึงคอมพิวเตอร์ได้โดยง่าย โดยผู้ใช้งานไม่รู้ตัว

คีย์ล็อกเกอร์ (Keylogger) โปรแกรมซึ่งบันทึกกิจกรรมการกดลงบนแป้นพิมพ์ที่ Keyboard เครื่องคอมพิวเตอร์ของผู้ใช้งาน ซึ่งจะส่งข้อมูลกิจกรรมการกดทุกครั้งนี้ ไปให้ผู้ไม่ประสงค์ดี ตามที่มีการตั้งค่าไว้ ซึ่งผู้ใช้งานโปรแกรมนี้ไม่ต้องอาศัยความรู้พิเศษแต่อาจสามารถคาดเดาห้สผ่านได้จากกระบวนการนี้

แบ็กดอร์ (Backdoors) มีความสามารถเปิดช่องทางเข้าสู่ระบบคอมพิวเตอร์หรือเครือข่าย ให้ผู้ที่ไม่หวังดี สามารถเข้ามาควบคุมเครื่องคอมพิวเตอร์ของผู้ใช้งาน เช่น สั่งลบหรือโอนย้ายข้อมูล รวมทั้งติดตั้งโปรแกรมต่างๆ เสมือนเป็นผู้ใช้งานระบบหรือคอมพิวเตอร์นั้นๆ

แรนซัมแวร์ (Ransomware) มัลแวร์เรียกค่าไถ่สร้างความเสียหายแก่ผู้ใช้งานคอมพิวเตอร์ โดยจะทำการเข้ารหัสลับไฟล์ข้อมูลภายในเครื่องคอมพิวเตอร์ของผู้ใช้งาน ดังภาพประกอบที่ 2.3



ภาพประกอบที่ 2.3 แรนซัมแวร์ พุ่งเป้า ภาคธุรกิจ เพิ่ม 363%

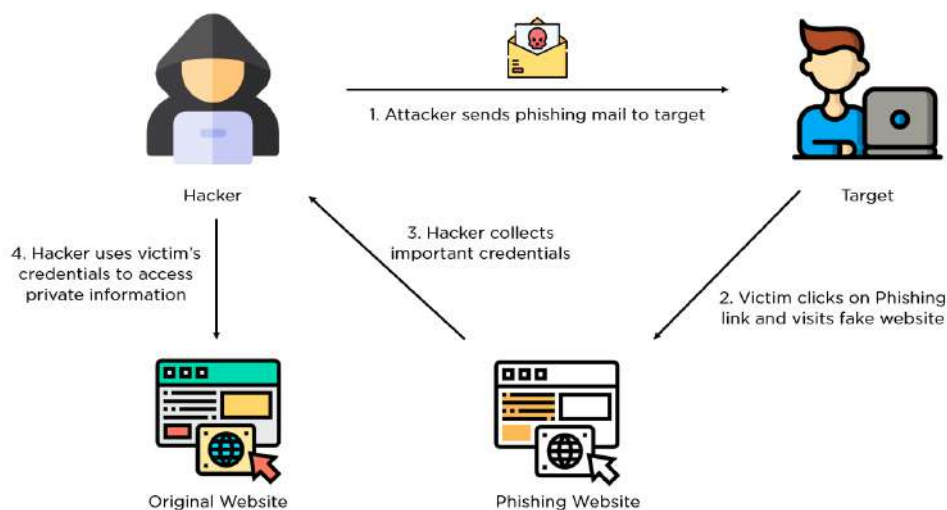
ที่มา : Facebook ETDA, 2562

จากภาพประกอบที่ 2.3 รายงานการเติบโตของ แรนซัมแวร์ ของ ETDA ซึ่งหากเมื่อถูกโจมตีแล้วจะทำให้ไม่สามารถเข้าถึงข้อมูลนั้น ๆ ได้ หลังจากนั้นจะแจ้งเตือนไปยังผู้ใช้งานคอมพิวเตอร์ เพื่อเรียกร้องเงินค่าไถ่กับการแลกเปลี่ยนให้ได้กุญแจถอดรหัสลับชุดข้อมูลที่มีการเข้ารหัสไว้ ซึ่งก็ไม่สามารถยืนยันได้ว่าหากมีการจ่ายค่าไถ่แล้วจะสามารถกู้คืนข้อมูลได้จริงตามที่กล่าวอ้างไว้

รายงานของบริษัท Malwarebytes สถิติตั้งแต่ไตรมาสที่สองของปี 2561 จนถึงไตรมาสที่สองของปี 2562 พบแรนซัมแวร์โจมตีหน่วยงานภาครัฐเพิ่มขึ้น 363% ในขณะที่การโจมตีผู้ใช้งานทั่วไปลดลง 12% สาเหตุเนื่องจากกลุ่มหน่วยงานภาครัฐมีโอกาสจ่ายเงินค่าไถ่มากกว่าผู้ใช้งานทั่วไป

2.1.2 Phishing Mail

Phishing เป็นคำพ้องเสียงจากคำว่า Fishing หมายถึงการตกปลา ซึ่งเป็นกลวิธีที่ผู้โจมตีใช้ในการหลอกลวงผู้เสียหายฟิชซิง เป็นคำที่ใช้เรียกเทคนิคการปลอมแปลงโดยใช้อีเมล หรือหน้าเว็บไซต์ปลอม ที่เหมือนว่าส่งมาจากหน่วยงานองค์กร หรือสถาบันที่มีชื่อเสียง เพื่อหลอกล่อผู้เสียหายให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่นๆเพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต ซึ่งทำให้เกิดความเสียหาย กระบวนการโจมตี ดังภาพประกอบที่ 2.4

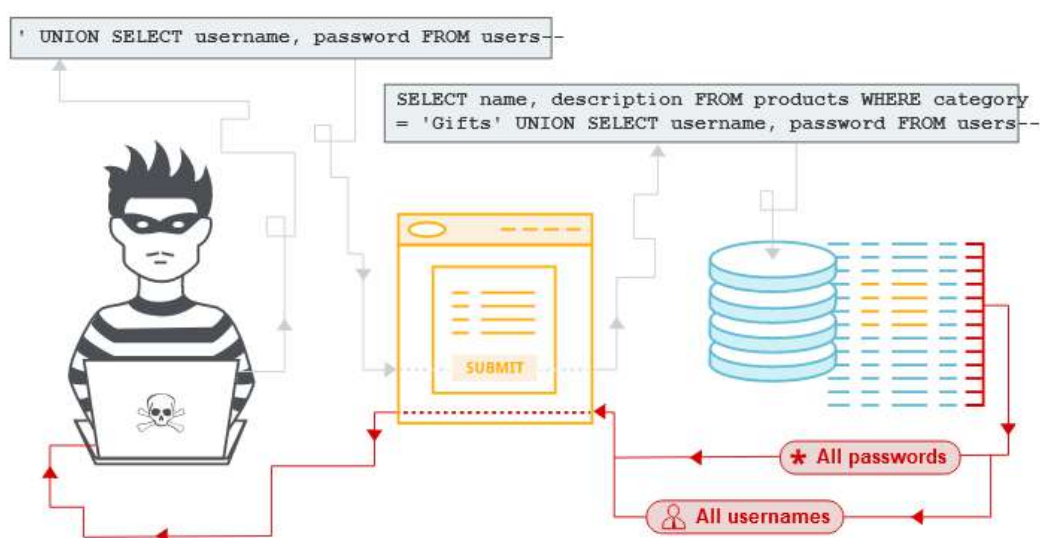


ภาพประกอบที่ 2.4 แสดงประเภทภัยคุกคาม Phishing Mail

ที่มา : Simplilearn, 2566

2.1.3 SQL Injection Attacks

SQL Injection Attacks (การโจมตี SQL Injection) เป็นเทคนิคการโจมตีที่ถูกใช้เพื่อการแทรกคำสั่งเพื่อเข้าถึงฐานข้อมูล (database) ผ่านการป้อนคำสั่ง SQL (Structured Query Language) เข้าสู่แอปพลิเคชันหรือเว็บไซต์ที่เชื่อมต่อกับฐานข้อมูล ซึ่งการโจมตี SQL Injection สามารถทำให้ผู้ไม่หวังดีเข้าถึงข้อมูลที่ไม่ควรเข้าถึงได้ หรือทำการคัดลอกข้อมูลต่างๆออกมาจากฐานข้อมูล หรือทำการแก้ไขข้อมูล ลบข้อมูล หรือทำอะไรก็ได้กับฐานข้อมูลตามที่สามารถทำได้ ขั้นตอนดังภาพประกอบที่ 2.5

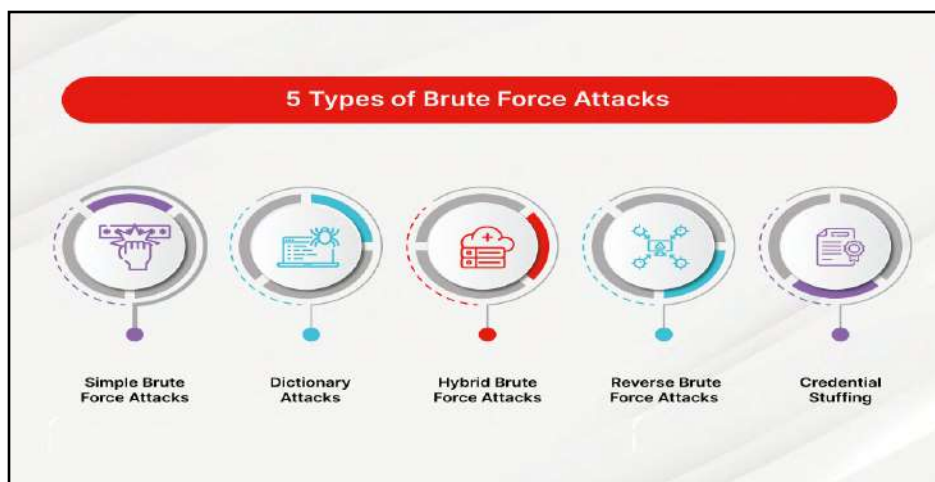


ภาพประกอบที่ 2.5 แสดงประเภทยุทธการ SQL Injection Attacks

ที่มา : Portswigger, 2566

2.1.4 Password Attacks

การโจมตีรหัสผ่าน (Password Attacks) เป็นแอปดักหรือเดารหัสผู้ใช้งานจากระบบบัญชีผู้ใช้งาน (User) ผ่านการให้บริการต่างๆ ผ่านเว็บไซต์ต่างๆ ที่ให้บริการอยู่มากในโลกออนไลน์ ซึ่งบางผู้ให้บริการก็ไม่มีมาตรฐานการตั้งรหัสผู้ใช้งาน (Password) ก็สามารถดักหรือเดารหัสผ่านที่ถูกตั้งไว้ได้อย่างง่าย ซึ่งในปัจจุบันก็มีเครื่องมือที่สามารถ ใช้ดักหรือคาดเดารหัสผ่านแบ่งออกเป็น 5 รูปแบบ จากข้อมูลจากเว็บไซต์ จากภาพประกอบที่ 2.6 ให้รายละเอียด ดังนี้



ภาพประกอบที่ 2.6 แสดงรูปแบบ Brute Force Attack

ที่มา : fortinet.com, พ.ศ. 2566

Simple Brute Force Attacks เป็นการโจมตีแบบ Brute Force แบบง่าย ๆ เกิดขึ้นเมื่อแฮ็กเกอร์พยายามเดาข้อมูลรับรองการเข้าสู่ระบบของผู้ใช้ด้วยตนเองโดยไม่ต้องใช้ซอฟต์แวร์ใดๆ โดยทั่วไปจะเป็นการใช้รหัสผ่านมาตรฐานหรือรหัสหมายเลขประจำตัวส่วนบุคคล (PIN)

การโจมตีเหล่านี้เกิดขึ้นได้ง่าย เนื่องจากผู้คนจำนวนมากยังคงใช้รหัสผ่านที่ไม่รัดกุม เช่น “รหัสผ่าน 123” หรือ “1234” หรือมีความคิดในการใช้รหัสผ่านที่ไม่ถูกต้อง เช่น การใช้รหัสผ่านเดียวกันสำหรับหลายเว็บไซต์ แฮ็กเกอร์ก็จะสามารถเดารหัสผ่านได้ซึ่งใช้การลาดตระเวนเพียงเล็กน้อยเพื่อถอดรหัสรหัสผ่านที่เป็นไปได้ของบุคคล เช่น ชื่อทีมกีฬาที่พวกเขาชื่นชอบ วันเดือนปีเกิด ชื่อคนรัก

Dictionary Attacks การโจมตีแบบพจนานุกรมเป็นรูปแบบพื้นฐานของการแฮ็กแบบ Brute force โดยผู้โจมตีจะเลือกเป้าหมาย จากนั้นทดสอบรหัสผ่านที่เป็นไปได้กับชื่อผู้ใช้ของบุคคลนั้น วิธีการโจมตีนี้ไม่ถือว่าการโจมตีแบบใช้ความรุนแรงในทางเทคนิค แต่สามารถก็มีความสำคัญในกระบวนการถอดรหัสรหัสผ่านของผู้โจมตีได้

ชื่อ “การโจมตีพจนานุกรม” ได้มาจากการที่แฮ็กเกอร์ที่เรียกใช้พจนานุกรมและแก้ไขคำด้วยอักขระพิเศษและตัวเลข การโจมตีประเภทนี้มักใช้เวลานาน และมีโอกาสสำเร็จต่ำเมื่อเปรียบเทียบกับวิธีการโจมตีที่ใหม่กว่า และมีประสิทธิภาพมากกว่า

Hybrid Brute Force Attacks การโจมตีแบบไฮบริดคือ เป็นการรวมวิธีการโจมตีแบบพจนานุกรมเข้ากับการโจมตีแบบธรรมดา โดยเริ่มต้นด้วยการที่ผู้โจมตีรู้ชื่อผู้ใช้ จากนั้นทำการโจมตีด้วยพจนานุกรม และวิธีการใช้เพื่อค้นหาชุดการเข้าสู่ระบบบัญชี

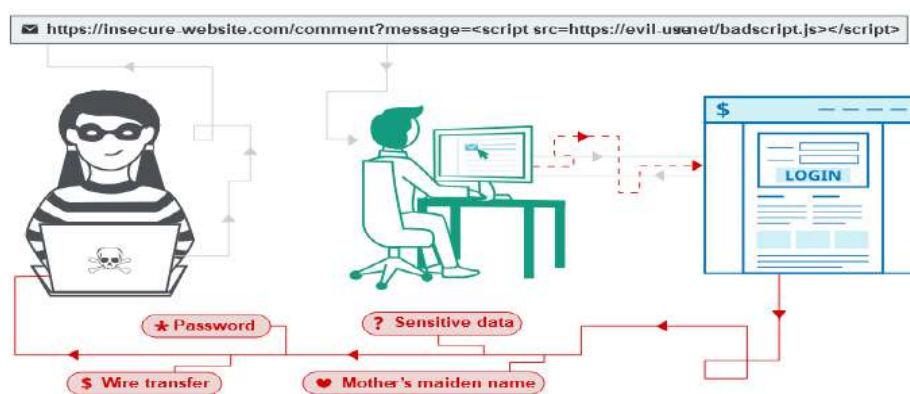
ผู้โจมตีจะเริ่มต้นด้วยรายการคำที่เป็นไปได้ จากนั้นทดลองผสมอักขระ ตัวอักษร และตัวเลข เพื่อค้นหารหัสผ่านที่ถูกต้อง วิธีการนี้ช่วยให้ค้นพบรหัสผ่านที่รวมคำทั่วไปหรือคำยอคนิยมเข้ากับตัวเลข ปี หรืออักขระแบบสุ่ม เช่น “Bangkok1234” หรือ “Manu2022”

Reverse Brute Force Attacks การโจมตีแบบทำให้ผู้โจมตีเริ่มต้นกระบวนการด้วยรหัสผ่านที่รู้จัก ซึ่งโดยทั่วไปจะถูกค้นพบผ่านการละเมิดเครือข่าย โดยใช้รหัสผ่านนั้นเพื่อค้นหาข้อมูลรับรองการเข้าสู่ระบบที่ตรงกันโดยใช้รายการชื่อผู้ใช้หลายล้านรายการ ผู้โจมตีอาจใช้รหัสผ่านที่ไม่รัดกุมที่ใช้กันทั่วไป เช่น “Password123” เพื่อค้นหาการจับคู่ในฐานข้อมูลชื่อผู้ใช้

Credential Stuffing การใส่ข้อมูลประจำตัวเป็นผลจากการใช้รหัสผ่านที่ไม่พึงระวังของผู้ใช้งาน ผู้โจมตีจะรวบรวมชื่อผู้ใช้และรหัสผ่านที่พวกเขาขโมยมา ซึ่งพวกเขาจะทดสอบบนเว็บไซต์อื่นเพื่อดูว่าพวกเขาสามารถเข้าถึงบัญชีผู้ใช้เพิ่มเติมได้หรือไม่ วิธีการนี้จะประสบความสำเร็จหากผู้คนใช้ชื่อผู้ใช้และรหัสผ่านเดียวกัน หรือใช้รหัสผ่านซ้ำสำหรับบัญชี และโปรไฟล์โซเชียลมีเดียต่างๆ

2.1.5 Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) เป็นรูปแบบของการโจมตีเว็บแอปพลิเคชันที่อนุญาตให้ผู้โจมตีแทรกสคริปต์ลงในหน้าเว็บที่เปิดใช้งานโดยผู้ใช้งานระบบที่อื่น ๆ ตามภาพประกอบที่ 2.7



ภาพประกอบที่ 2.7 แสดงประเภทภัยคุกคาม Cross-Site Scripting (XSS)

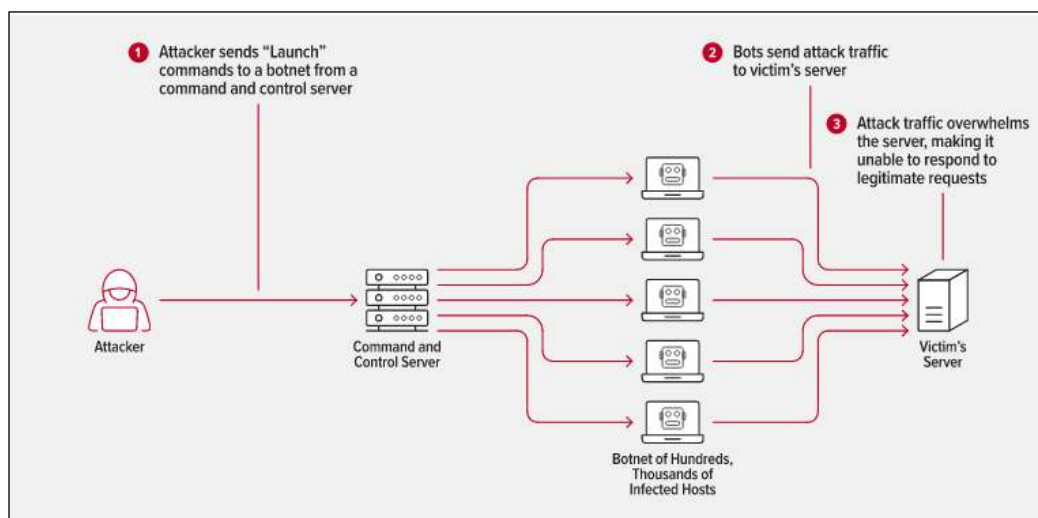
ที่มา : Portswigger.com, 2566

ซึ่งจะถูกทำให้รันในคอนเทนต์ของเว็บไซต์หรือแอปพลิเคชันอื่น ๆ ที่ถูกเข้าถึงผ่านเว็บเบราว์เซอร์ของผู้ใช้ระบบ XSS มีลักษณะที่ว่าโค้ดที่รันจะถูกทำให้รันในเบราว์เซอร์ของผู้ใช้ระบบคนอื่น ๆ แทนที่จะถูกรันในเซิร์ฟเวอร์หลักการของ Cross-Site Scripting (XSS) ช่องโหว่ในแอปพลิเคชัน XSS เกิดขึ้นเมื่อแอปพลิเคชันไม่ตรวจสอบหรือกรองข้อมูลที่ผู้ใช้ป้อนค่า และส่งค่ามาที่เว็บเบราว์เซอร์หรือแสดงบนหน้าเว็บไซต์ โดยไม่รักษาค่าความมั่นคงปลอดภัยได้

แท็กสคริปต์ (Script Injection) ผู้โจมตีส่งข้อมูลชุดสคริปต์ที่มีโค้ด JavaScript ผ่านแอปพลิเคชัน (เช่น การส่งความคิดเห็น) และทำให้บนหน้าเว็บเบราว์เซอร์ของผู้ใช้ระบบอื่น ๆ รันสคริปต์นั้น ๆ ซึ่งมีผลเปลี่ยนแปลงหน้าเว็บหรือโอนข้อมูลสำคัญ

2.1.6 Distributed Denial-of-Service (DDoS)

การโจมตีแบบ Distributed Denial-of-Service (DDoS) เป็นวิธีการที่ผู้โจมตีพยายามทำให้เว็บไซต์หรือเซิร์ฟเวอร์ไม่สามารถให้บริการผู้ใช้ได้อย่างปกติโดยการนำส่งข้อมูลหรือการจัดการจราจรข้อมูล (Traffic) ที่มากเกินไปเพื่อทำให้ระบบหรือเซิร์ฟเวอร์หน่วยประมวลผลทำงานผิดปกติหรือหยุดชะงัก ซึ่งมักใช้กับคอมพิวเตอร์เป็นจำนวนมากหรือเป็นอุปกรณ์เครือข่ายต่าง ๆ ในการส่งข้อมูลที่ทำให้เซิร์ฟเวอร์ถูกขัดจังหวะการทำงานในขณะใดขณะหนึ่ง ดังภาพประกอบที่ 2.8

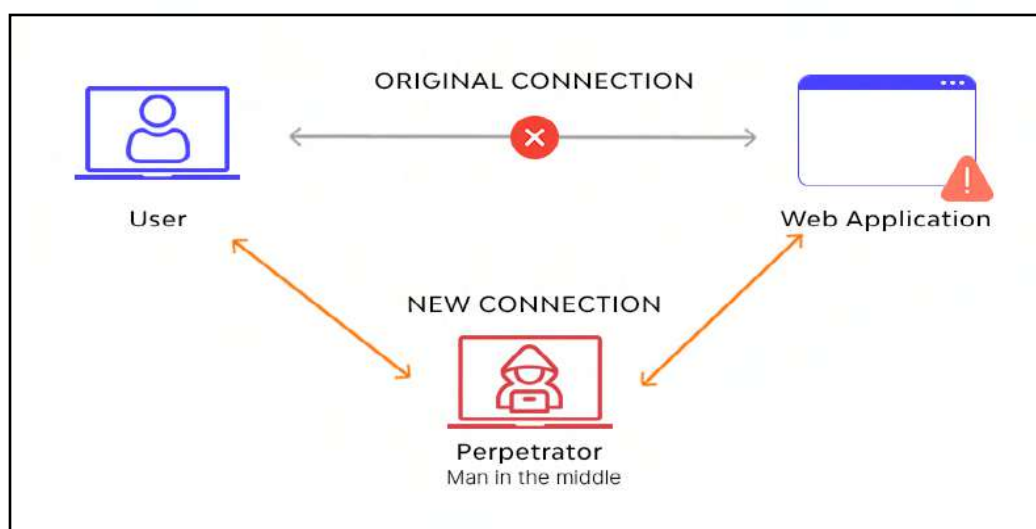


ภาพประกอบที่ 2.8 แสดงประเภทภัยคุกคาม Distributed Denial-of-Service (DDoS)

ที่มา : Nginx, 2566

2.1.7 Man-in-the-Middle Attacks

Man-in-the-Middle Attacks (MitM Attacks) หมายถึงการโจมตีที่อยู่ตรงกลางระหว่างสองส่วนที่กำลังสื่อสารกัน และสามารถดักจับการสื่อสารนี้ได้เป็นอย่างดี ในการโจมตีแบบ Man-in-the-Middle ผู้โจมตีจะซ่อนตัวเอง และตรวจจับข้อมูลที่ส่งหรือรับข้อมูลที่ผ่านการสื่อสารที่มีการดักจับข้อมูลอยู่ โดยที่ผู้สื่อสารระหว่างกันจะไม่มีใครทราบใดๆ ทำให้ผู้สื่อสารสองฝ่ายไม่รู้ว่า มีผู้ตรวจจับกลางระหว่างเครื่องของพวกเขา รายละเอียดดังภาพประกอบที่ 2.9



ภาพประกอบที่ 2.9 แสดงประเภทภัยคุกคาม Man-in-the-Middle Attacks

ที่มา : Wallarm.com, 2566

แนวคิดเกี่ยวกับภัยคุกคามทางไซเบอร์สามารถนำศึกษาเพื่อใช้เพื่อเป็นการตรวจจับ ป้องกัน และตอบสนองต่อการคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในระบบแม่ข่ายหรือลูกข่าย เพื่อให้เกิดความมั่นคงปลอดภัยได้มากขึ้น รวมถึงการใช้มาตรฐานการรักษาความมั่นคงปลอดภัยเพื่อลดความเสี่ยง และควบคุมความเสี่ยงในสถานะที่อาจเกิดการโจมตีระบบ และเพื่อการเชื่อมั่นการให้บริการที่ต้องพร้อมอยู่เสมอ ถึงแม้ว่า อาจจะไม่มียระบบป้องกันใดดีที่สุด แต่การประเมิน วิเคราะห์ ป้องกัน ยังคงเป็นแนวทางที่นำมาปรับใช้เพื่อลดความเสี่ยงหรือช่องโหว่ของระบบ จนถึงปัจจุบัน

2.2 แนวคิดเกี่ยวกับการโจมตีทางไซเบอร์

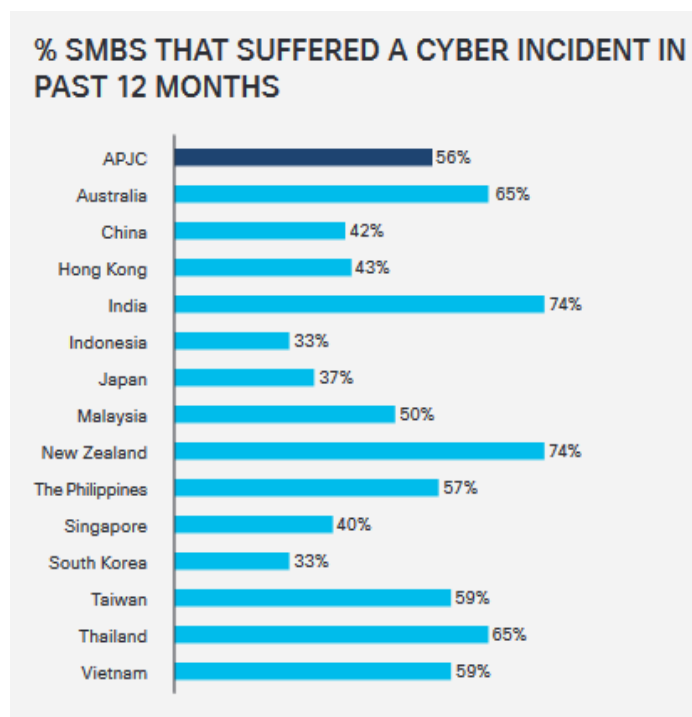
การโจมตีทางไซเบอร์เป็นกิจกรรมที่ผู้ไม่ประสงค์ดีใช้เทคนิคและเครื่องมือต่าง ๆ เพื่อเข้าถึงระบบคอมพิวเตอร์ เครือข่าย และข้อมูลทางดิจิทัลของผู้อื่นๆ โดยไม่ได้รับอนุญาต การโจมตีทางไซเบอร์สามารถมีลักษณะ และวัตถุประสงค์หลายแบบ เช่น จุดประสงค์ทางการเมือง อาชญากรรม หรือส่วนตัว ในการทำลายหรือเข้าถึงข้อมูลที่เป็นความลับ ความรุนแรงและกว้างขวางของการโจมตีทางไซเบอร์ทำให้เราต้องสนใจและระมัดระวังตลอดเวลา การโจมตีทางไซเบอร์บนแพลตฟอร์มโซเชียลมีเดีย และเว็บไซต์ที่เก็บข้อมูลส่วนบุคคลอาจมีผลกระทบรุนแรงต่อประชากรทั่วไปและองค์กรต่าง ๆ ไม่ว่าจะเป็นในด้านธุรกิจ ภาครัฐ หรือองค์กรไม่แสวงหากำไร นี่คือการประเมินสำคัญที่ควรพิจารณา

2.2.1 ความเสี่ยงของข้อมูลส่วนบุคคล

การโจมตีทางไซเบอร์ที่เป้าหมายเป็นข้อมูลส่วนบุคคลมีความสำคัญเนื่องจากมีผลกระทบต่อความเป็นส่วนตัวของบุคคลเป็น การละเมิดข้อมูลส่วนบุคคลซึ่งตามประกาศ (คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล 2565) หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าใช้งาน ปรับเปลี่ยนแปลง การแก้ไข หรือแสดงข้อมูลที่เกี่ยวข้องกับส่วนบุคคลโดยมิได้อำนาจหรือโดยมิชอบ ไม่ว่าจะเป็นเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด ซึ่งอาจนำไปสู่การละเมิดความเป็นส่วนตัวและการประพฤติดิตตามกฎหมาย

2.2.2 ความเสี่ยงการดำเนินงานทางธุรกิจ SME

ข้อมูลธุรกิจอาจมีความเสี่ยงต่าง ๆ ที่อาจส่งผลกระทบต่อองค์กรความเสี่ยงเหล่านี้ ได้แก่ ความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล เช่น การรั่วไหล การโจรกรรม การสูญหาย การบิดเบือน การปลอมแปลง การทำลาย การคัดลอก และการปิดกั้นข้อมูล ซึ่งมากกว่า 65% ของ SME ในประเทศไทยจะถูกโจมตีทางไซเบอร์ โดยผลการวิจัยในปีที่ผ่านมาจาก Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense (Cisco, 2021) ในปี 2021 ซึ่งได้กล่าวถึงธุรกิจขนาดเล็ก และขนาดกลาง Small and Medium Sized Businesses (SMBs) ตามภาพประกอบที่ 2.10



ภาพประกอบที่ 2.10 แสดง SMB ประสบเหตุการณ์ทางไซเบอร์

ที่มา : Cisco, 2021

การประสบปัญหาการดำเนินงานหยุดชะงักเนื่องจากการโจมตีทางไซเบอร์ และสร้างความเสียหายต่อธุรกิจมูลค่าอย่างน้อย 17 ล้านบาทจำนวน 47% และมูลค่ากว่า 34 ล้านบาท จำนวน 28% ซึ่งสาเหตุสำคัญที่สุดของธุรกิจ SME ถูกโจมตี จากมัลแวร์เป็นอันดับที่หนึ่งอยู่ที่ 91% และการโจมตีในรูปแบบฟิชชิง (Phishing) เป็นอันดับที่สองอยู่ที่ 77% สาเหตุหลักมาจากโซลูชันด้านความมั่นคงปลอดภัย Cyber Security ไม่มีประสิทธิภาพเพียงพอในการตรวจจับ หรือป้องกันการโจมตีจากภัยคุกคามทางไซเบอร์ได้ ซึ่งในขณะอีก 25% มาจากสาเหตุหลักที่ไม่ได้ติดตั้งระบบป้องกันด้านความมั่นคงปลอดภัย Cyber Security หรือไม่ให้ความสำคัญด้านความมั่นคงปลอดภัยเพียงพอ หากบริษัทที่ถูกโจมตีจนสูญเสียข้อมูลของลูกค้า หรือข้อมูลของพนักงาน อีกทั้งบริษัทที่ถูกโจมตีมีความแตกต่างกันไป ดังนั้นธุรกิจจำเป็นต้องดำเนินการปิดช่องโหว่ไม่ให้ผู้อื่นเข้ามาโจมตีระบบสารสนเทศ และให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางข้อมูลแก่บุคลากรในองค์กร ซึ่งเป็นสิ่งสำคัญ ที่ต้องทำความเข้าใจกับการดูแลและตรวจสอบระบบอยู่เสมอ

2.2.3 การละเมิดความเป็นส่วนตัว

การโจมตีทางไซเบอร์บนโซเชี่ยลมีเดียสามารถทำให้ข้อมูลส่วนบุคคลหรือสิทธิของบุคคลถูกเปิดเผยหรือถูกใช้ในทางที่ไม่เหมาะสม จากแนวคิด การละเมิดความเป็นส่วนตัวทางไซเบอร์เป็นความกังวลที่สำคัญในยุคดิจิทัลการใช้อุปกรณ์อัจฉริยะ และ (Internet of Things) ที่เพิ่มขึ้นทำให้ช่องโหว่ทางไซเบอร์เพิ่มขึ้น และอาจเกิดการละเมิดข้อมูลส่วนบุคคล และการละเมิดเหล่านี้มักเชื่อมโยงกับการละเมิดความเป็นส่วนตัวทางเพศเนื่องจากความรุนแรงทางเพศที่อำนวยความสะดวกโดยเทคโนโลยี และการบุกรุกความเป็นส่วนตัวทางอิเล็กทรอนิกส์เชื่อมโยงกัน ได้มีความเห็นว่า ความรุนแรงทางเพศที่อำนวยความสะดวกโดยเทคโนโลยีในยุคดิจิทัลเป็นการละเมิดที่ขยายวัฒนธรรมการข่มขืนยุคแอนะล็อกและการละเมิดความเป็นส่วนตัวทางเพศ และข้อมูลนั้นเชื่อมโยงกันในยุคดิจิทัล และได้มีความเห็นว่า กฎหมายไซเบอร์ในยุคสมัยใหม่อาจบุกรุกความเป็นส่วนตัวของบุคคล และให้บริการผลประโยชน์ของผู้ที่ออกกฎหมายแทนที่จะปกป้องสาธารณชน มีความเห็นเช่นกันว่าอาชญากรรมสินเชื่อนอนไลน์ไม่เพียง แต่เป็นเรื่องของอาชญากรรมไซเบอร์เท่านั้น แต่ยังเกี่ยวข้องกับการละเมิดสิทธิมนุษยชน และการละเมิดสิทธิความเป็นส่วนตัวด้วยการใช้ประโยชน์จากข้อมูลส่วนบุคคลของผู้ดูแลและการกระทำหาวาดกลัวต่อผู้ดูแลและครอบครัวของพวกเขาเป็นบางส่วนของผลกระทบทางอาญาที่เกี่ยวข้องกับสินเชื่อนอนไลน์และ มีความเห็นเช่นเดียวกัน หลักคำสอนความเป็นส่วนตัวสำหรับยุคไซเบอร์ต้องกล่าวถึงการใช้ข้อมูลส่วนบุคคลทุกข้อมูมิซึ่งก่อให้เกิดภัยคุกคามอย่างมีนัยสำคัญต่อความเป็นส่วนตัว กฎหมายที่มีอยู่และศาลไม่ได้สร้างหลักคำสอนเกี่ยวกับความเป็นส่วนตัวที่สอดคล้องกัน และไม่ตอบสนองต่อความท้าทายที่เป็นเอกลักษณ์ของยุคไซเบอร์อย่างเพียงพอ

2.2.4 การควบคุมการเข้าถึงข้อมูล

การควบคุมการเข้าถึงข้อมูลไซเบอร์เป็นแง่มุมที่สำคัญในการรับประกันความมั่นคงปลอดภัย และความเป็นส่วนตัวของข้อมูลในระบบต่างๆระบบทางกายภาพทางไซเบอร์ทางการแพทย์ในปัจจุบันเผชิญกับความท้าทายในแง่ของการแบ่งปันข้อมูล ความสม่ำเสมอ การกำหนดมาตรฐาน การป้องกัน และการรั่วไหล เพื่อแก้ไขปัญหเหล่านี้ มีการเสนอกลไกการควบคุมการเข้าถึงที่ใช้บล็อกเชน ซึ่งจำแนกข้อมูลทางการแพทย์ กำหนดระดับน้ำหนัก และกำหนดกลยุทธ์การควบคุมการเข้าถึง ในทำนองเดียวกัน ในบริบทของ Cyber Physical Social Systems (CPSS) มีการเสนอโครงการควบคุมการเข้าถึงที่ใช้บล็อกเชนที่เรียกว่า BaccPSS เพื่อรักษาความมั่นคงปลอดภัยข้อมูลขนาดใหญ่ของ CPSS และปกป้องความเป็นส่วนตัว สุดท้ายนี้มีการแนะนำวิธีการควบคุมการเข้าถึงข้อมูล และอุปกรณ์เพื่อปรับปรุงการใช้พลังงานของระบบ และการประมวลผลการเข้าถึงข้อมูล

2.2.5 การเข้าใจและการตระหนัก

ผู้ใช้ควรรู้จักความมั่นคงปลอดภัยและองค์กรควรให้ความรู้แก่พนักงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์และเสมือนจริง ตามที่อธิบายว่า การรับรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์หมายถึงระดับความชื่นชมความเข้าใจหรือความรู้เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์หรือด้านความมั่นคงปลอดภัยของข้อมูลซึ่งรวมถึงการตระหนักถึงความเสี่ยงทางไซเบอร์ ภัยคุกคาม และมาตรการป้องกันที่เหมาะสม ความจำเป็นของความมั่นคงปลอดภัยทางไซเบอร์ผ่านกลยุทธ์การศึกษาและการป้องกัน ซึ่งมีการเสนอแนวทางเช่น การพัฒนาแพลตฟอร์มเกมสำหรับการศึกษาด้านความมั่นคงปลอดภัยทางไซเบอร์ Cyber Awareness Learning Imitation Environment (CALIE) ซึ่งรวมถึงการเรียนรู้เกี่ยวกับการโจมตีทางไซเบอร์และกลไกการป้องกันต่างๆ และเป็นทางเลือกที่ดีกว่าสำหรับการให้ความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ ที่ไม่ใช่ด้านไอทีและไม่ใช่มืออาชีพ ตามงานวิจัยของ รวมถึงใช้เครื่องมือตรวจจับการบุกรุก (IDS) ยังคงมีบทบาทในการสร้างความตระหนักถึงสถานการณ์ทางไซเบอร์โดยให้คำแนะนำแก่ผู้ดูแลระบบ โดยรวมแล้วความเข้าใจ และการรับรู้ทางไซเบอร์มีความสำคัญต่อบุคคล และองค์กรในการลดความเสี่ยง และผลกระทบจากการโจมตีทางไซเบอร์

2.2.6 การรายงานและการตอบสนองต่อการละเมิด

องค์กรควรมีกระบวนการรายงานและการตอบสนองต่อการละเมิดที่มีประสิทธิภาพเพื่อที่จะตรวจสอบ และรับมือกับการโจมตีทางไซเบอร์ การรายงาน และการตอบสนองต่อการละเมิดทางไซเบอร์เป็นแง่มุมที่สำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์องค์กรจำเป็นต้องเข้าใจลักษณะ และความสำคัญของภัยคุกคามที่พวกเขาเผชิญและใช้มาตรการที่เหมาะสมเพื่อรักษาความมั่นคงปลอดภัย เพื่อที่จะตอบสนองต่อการละเมิดความมั่นคงปลอดภัยอย่างมีประสิทธิภาพ สิ่งสำคัญคือต้องมียุทธศาสตร์ที่เป็นทางการที่ครอบคลุมความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ นอกจากนี้ สิ่งสำคัญคือต้องมีกลไกในการรับการแจ้งเตือนเกี่ยวกับการละเมิดความมั่นคงปลอดภัย และเพื่อระบุบัญชีผู้ใช้ที่อาจได้รับผลกระทบทันที เมื่อมีการระบุการละเมิดองค์กรควรดำเนินการด้านความมั่นคงปลอดภัยทันทีเพื่อแก้ไขการละเมิด และบรรเทาผลกระทบ นอกจากนี้ยังเป็นสิ่งสำคัญที่จะต้องทำการวิเคราะห์เชิงปริมาณ และเชิงคุณภาพของเหตุการณ์การละเมิดเพื่อรับข้อมูลเชิงลึกเกี่ยวกับความถี่ของเหตุการณ์การหยุดชะงัก และเพื่อแจ้งการพัฒนายุทธศาสตร์ในอนาคต ด้วยการดำเนินการตามมาตรการเหล่านี้ องค์กรสามารถเพิ่มความสามารถในการรายงาน และตอบสนองต่อการละเมิดทางไซเบอร์ได้อย่างมีประสิทธิภาพ

2.2.7 การใช้มาตรฐานและเนื้อหาเกี่ยวกับความมั่นคงปลอดภัย

การใช้มาตรฐาน และเนื้อหาความมั่นคงปลอดภัยทางไซเบอร์เป็นสิ่งสำคัญในการสร้างความมั่นใจในความมั่นคงปลอดภัยของระบบสารสนเทศ และการป้องกันภัยคุกคามทางไซเบอร์องค์กรจำเป็นต้องใช้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์เพื่อรักษาความมั่นคงปลอดภัยสินทรัพย์ของตน และลดความเสี่ยงที่เกิดจากอาชญากรรมทางไซเบอร์ มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ให้ชุดข้อกำหนดที่ระบบ และข้อมูลต้องบรรลุ และการปฏิบัติตามมาตรฐานเหล่านี้เป็นสิ่งจำเป็นสำหรับทุกองค์กร นอกจากนี้การรวมหลักการ และแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์เข้ากับหลักสูตรระบบสารสนเทศเป็นสิ่งจำเป็นเพื่อปรับปรุงการศึกษาด้านความมั่นคงปลอดภัยทางไซเบอร์ และเตรียมผู้เชี่ยวชาญในอนาคต ระบบการฝึกอบรมที่ใช้สื่อ และการฝึกอบรมสามารถช่วยให้ผู้ใช้จดจำ และตอบสนองต่อภัยคุกคามด้านความมั่นคงปลอดภัยได้อย่างเหมาะสม และการปรับแต่งระบบเหล่านี้ด้วยเนื้อหาที่มีตราสินค้าสามารถเพิ่มประสิทธิภาพได้ การสนับสนุนทางกฎหมายสำหรับความมั่นคงปลอดภัยทางไซเบอร์ก็มีความสำคัญเช่นกันและประเทศต่างๆ และองค์กรระหว่างประเทศได้กำหนดกรอบ และมาตรฐานขององค์กรเพื่อแก้ไขปัญหาคความมั่นคงปลอดภัยทางไซเบอร์ โดยรวมแล้วการใช้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์และเนื้อหาเป็นสิ่งจำเป็นสำหรับการป้องกันภัยคุกคามทางไซเบอร์และรับประกันความมั่นคงปลอดภัยของระบบสารสนเทศ การรับรองตัวเองตามมาตรฐานความมั่นคงปลอดภัยเช่น ISO 27001, ISO 27017, ISO 27701และการใช้นโยบายความมั่นคงปลอดภัยที่เหมาะสม

2.3 แนวคิดเกี่ยวกับอาชญากรรมทางไซเบอร์

อาชญากรรม ความหมายตามพจนานุกรมฉบับราชบัณฑิตยสถาน อาชญากรรม หมายถึง การกระทำความผิดทางอาญา แม้คำของ “อาชญากรรม” คือ อาชญา และส่วนภาษาอังกฤษซึ่งมีความหมายตรงกับคำว่า Crime

อาชญากรรม คือ การกระทำความผิดทางอาญา ซึ่งเป็นปัญหาของสังคมอย่างหนึ่งที่มีผลกระทบต่อความมั่นคงปลอดภัยในชีวิต และสินทรัพย์เป็นจำนวนมาก โดยการกระทำความผิดทางอาญานั้น ได้กระทำขึ้นโดย “อาชญากร” เช่น คดีฆ่าผู้อื่น ทำร้ายร่างกาย ข่มขืนกระทำชำเรา ลักทรัพย์ วิ่งราวทรัพย์ ชิงทรัพย์ และปล้นทรัพย์ เป็นต้น

อาชญากรรมไซเบอร์ (Cybercrime) หมายถึง อาชญากรรมที่กระทำโดยใช้เทคโนโลยีสารสนเทศ และการสื่อสารเช่นคอมพิวเตอร์และอินเทอร์เน็ตเป็นคำที่กว้างขวางซึ่งครอบคลุมกิจกรรมที่ผิด

กฎหมายต่าง ๆ รวมถึงการฉ้อโกง การโจรกรรม การกระตุ้นความรุนแรง การกระทำความผิดที่ไม่เหมาะสม แบบลึกลับ การโจรกรรมลิขสิทธิ์ ข่วปลอม และการก่อการร้าย ตามนิยามของ ได้ข้อสรุปอีกว่า การต่อสู้กับอาชญากรรมไซเบอร์เป็นสหวิทยาการที่รวมองค์ประกอบจากสาขาต่าง ๆ เช่นกฎหมาย อาญาอาชญากรวิทยานิติวิทยาศาสตร์กฎหมายระหว่างประเทศกระบวนการทางอาญากฎหมายการปกครอง และกฎหมายแพ่งความซับซ้อน และความหลากหลายมิติของอาชญากรรมไซเบอร์จำเป็นต้องมีแนวทางที่ครอบคลุมในการทำความเข้าใจ ซึ่งเปรียบเทียบสถิติปี 2561 ถึงปี 2562 จากภาพประกอบที่ 2.11



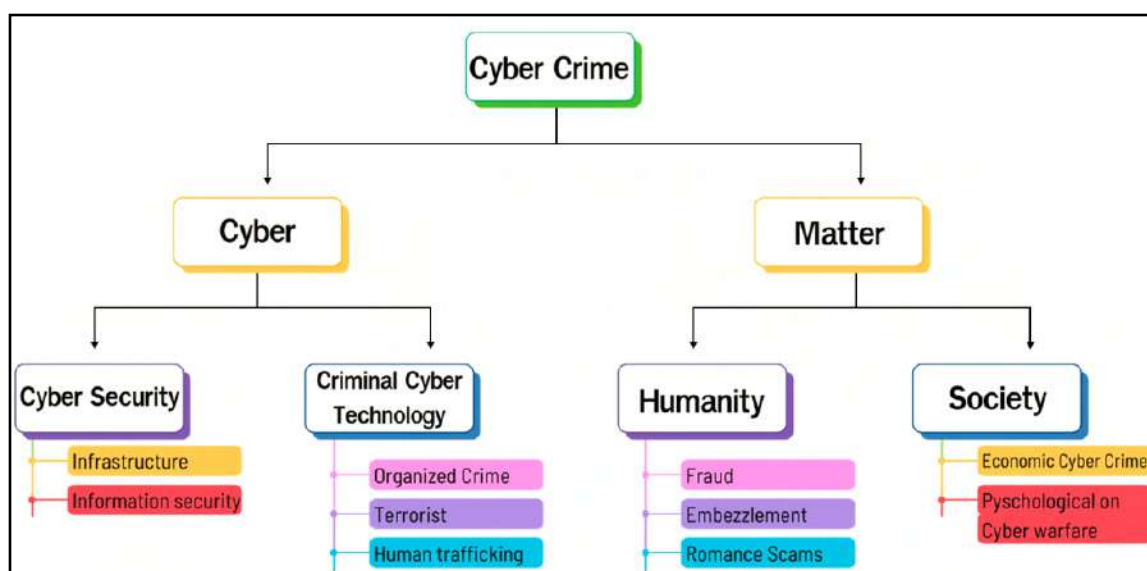
ภาพประกอบที่ 2.11 แสดงสถิติคดีอาชญากรรมทางเทคโนโลยี

ที่มา : Prachachat.net, 2562

2.3.1 ประเภทของอาชญากรรมทางไซเบอร์

อาชญากรรมทางไซเบอร์ครอบคลุมความผิด และการกระทำผิดที่เกี่ยวข้องกับคอมพิวเตอร์ หรือเครื่องมือสื่อสารเป็นเป้าหมายหรือเครื่องมือการดำเนินการอาชญากรรมทางไซเบอร์ประเภททั่วไป ได้แก่ สื่อบริการเด็ก การสืบค้นทางไซเบอร์ การขโมยข้อมูลประจำตัว การฟอกข้อมูลทางไซเบอร์ การขโมยบัตรเครดิต การก่อการร้ายทางไซเบอร์ การขายยาเสพติด การรั่วไหลของข้อมูล เนื้อหาที่ชัดเจนทางเพศ ฟิชชิง และการแฮ็กไซเบอร์ การพึ่งพาเทคโนโลยี และอินเทอร์เน็ตที่เพิ่มขึ้นทำให้เกิดการโจมตี

ทางไซเบอร์ และการละเมิดข้อมูลบ่อย และซับซ้อนมากขึ้นภัยคุกคามทางไซเบอร์ที่พบบ่อยที่สุดบางประเภท ได้แก่ มัลแวร์ ฟิชซิง และแรนซัมแวร์ นอกจากนี้ยังมีอาชญากรรมไซเบอร์ประเภทต่าง ๆ ที่สามารถจัดประเภทเป็นอาชญากรรมไซเบอร์ทางเศรษฐกิจและสังคม (เช่น การฉ้อโกงออนไลน์) และอาชญากรรมทางไซเบอร์ทางจิตสังคม (รวมถึงการกลั่นแกล้งทางไซเบอร์ สื่อลามก แก๊งแค้น และการล่วงละเมิดออนไลน์) ผู้หญิงมักจะรับรู้ถึงอาชญากรรมทางไซเบอร์ทางจิตสังคมแย่กว่าผู้ชาย ในขณะที่ไม่มีความแตกต่างทางเพศในการรับรู้เกี่ยวกับอาชญากรรมทางไซเบอร์ทางเศรษฐกิจและสังคม โดยอาจจะแบ่งประเภทของอาชญากรรมทางไซเบอร์ ซึ่งได้ทำการแยกแยะแบ่งเปรียบเทียบพร้อมรายละเอียดเป็น 2 ประเภท ดังภาพประกอบที่ 2.12



ภาพประกอบที่ 2.12 แสดงแบ่งประเภทของอาชญากรรมทางไซเบอร์
ที่มา : ประเมศวร์ กุมารบุญ, 2561

1. อาชญากรรมทางไซเบอร์ที่มีผลต่อวัตถุ

อาชญากรรมไซเบอร์ที่มุ่งเป้าไปที่การโจมตีคอมพิวเตอร์กลายเป็นความกังวลที่สำคัญเนื่องจากวิวัฒนาการอย่างรวดเร็วของเทคโนโลยี และความซับซ้อนที่เพิ่มขึ้นของภัยคุกคามทางไซเบอร์องค์กรกำลังเผชิญกับความท้าทายในการป้องกันการโจมตีประเภทต่างๆ รวมถึงไวรัสคอมพิวเตอร์การโจมตีโครงสร้างพื้นฐานเครือข่าย และการโจมตีทางไซเบอร์ที่แพร่กระจายผ่านเครือข่ายคอมพิวเตอร์

นักวิจัยได้พัฒนาแบบจำลองการคำนวณ และเทคนิคการจำลองเพื่อศึกษาการแพร่กระจายของการโจมตีทางไซเบอร์ในเครือข่ายคอมพิวเตอร์ และเพื่อตรวจสอบประสิทธิภาพของกลไกการป้องกันจากแบบจำลองโจมตีทางไซเบอร์กำลังเพิ่มขึ้นทั้งในแง่ของความเร็วและความซับซ้อน โดยผู้โจมตีพัฒนาวิธีการใหม่ ๆ เพื่อใช้ประโยชน์จากเครือข่ายโปรแกรมและข้อมูลอย่างต่อเนื่อง เพื่อต่อสู้กับอาชญากรรมทางไซเบอร์อย่างมีประสิทธิภาพมีความจำเป็นในการรับรู้และความร่วมมือระดับโลกเนื่องจากผู้โจมตีสามารถดำเนินการข้ามพรมแดนระหว่างประเทศ บุคคล บริษัท และหน่วยงานมีความรับผิดชอบร่วมกันในการรับประกันความมั่นคงปลอดภัยของข้อมูล และความเป็นส่วนตัวของข้อมูล และควรประเมิน และพัฒนามาตรการรักษาความมั่นคงปลอดภัยของตนเอง

2. อาชญากรรมทางไซเบอร์ที่มีผลต่อจิตใจ

อาชญากรรมทางไซเบอร์ใช้เทคโนโลยีการสื่อสารเพื่อกระทำความผิดที่เน้นไปที่จิตใจของบุคคล เช่น คดีโรแมนซ์ (Romance scams) ผ่านโซเชียลมีเดีย ซึ่งหลอกลวงผู้ใช้ให้ตกหลุมรักออนไลน์แล้วเสียเงินหรือแชร์ข้อมูลส่วนตัว การปฏิบัติคดีนี้ถือโกง การล่อลวง หรือการกลั่นแกล้งทางไซเบอร์ (Cyber Bullying) ในรูปแบบของการกลั่นแกล้งและข่มเหงออนไลน์ จากสถิติดังภาพประกอบที่ 2.13



ภาพประกอบที่ 2.13 แสดงสถิติ Cyber Bullying ระดับชั้น ม.1-ม.3 ปี 2560

ที่มา : Thai Media Fund, 2564

หากเป็นระดับสังคม เช่น ข่าวดลอกหลวง หรือ Psychological Cyber Warfare คือการใช้สื่ออินเทอร์เน็ตเพื่อเพาะเมล็ดความสับสนในสังคม โดยการแข่งขันเนื้อหาเพื่อทำให้คนในสังคมเข้าใจในทิศทางที่ต้องการ การใช้เนื้อหาเพื่อปลุกระดมทางการเมืองหรือสร้างอาชญากรรมแห่งความเกลียดชัง (Hate Crime) ที่เป็นอันตราย มีเป้าหมายในการสร้างความแตกแยก และทำลายล้างความมั่นคงของชาติ ซึ่งถือเป็นรูปแบบของอาชญากรรมไซเบอร์ที่รุนแรงที่สุด ด้วยสถิติ Hate Crime ในประเทศสหรัฐอเมริกา จากภาพประกอบที่ 2.14



ภาพประกอบที่ 2.14 แสดงสถิติ Hate Crime 20 รัฐใหญ่ ประเทศสหรัฐอเมริกา 2015

ที่มา : Waymagazine.org, 2559

2.3.2 อาชญากรรมทางไซเบอร์กับทฤษฎีอาชญาวิทยา

ทฤษฎีอาชญาวิทยาถูกนำไปใช้ในการศึกษาอาชญากรรมไซเบอร์ แต่ผลลัพธ์นั้นมีการผสมผสาน ทฤษฎีอาชญากรรมแบบดั้งเดิมถูกนำมาใช้เพื่อทำความเข้าใจการกระทำผิด และการตกเป็นเหยื่อประเภทต่างๆ ทฤษฎี Response Styles Theory (RST) คิดโดย (Nolen-Hoeksema, 1998) เป็นกรอบสำหรับการอธิบายอาชญากรรมทางไซเบอร์ และพบว่าลักษณะที่เกี่ยวข้องกับเชื่อมโยงทฤษฎีอาชญากรรมสอดคล้องกับความผิด และการตกเป็นเหยื่ออาชญากรรมไซเบอร์ประเภทต่างๆ และชี้ให้เห็นถึงความต้องการทฤษฎีแบบบูรณาการทางไซเบอร์ทั่วไป จากข้อสรุปของ (Adam Bossler, 2019) ทฤษฎีอาชญากรรมมีส่วนสำคัญต่อความเข้าใจของเราเกี่ยวกับการกระทำผิด และการตกเป็น

เหยื่ออาชญากรรมทางไซเบอร์ หลักฐานเชิงประจักษ์ที่ทบทวนในบทความแสดงให้เห็นถึงความสามารถของทฤษฎีอาชญากรรมแบบดั้งเดิมกับอาชญากรรมไซเบอร์ประเภทต่าง ๆ และการศึกษาของ (Anne-Marie Mohammed¹, Vladlena Benson², George Saridakis, 2020) การป้องกันอาชญากรรมมีประสิทธิภาพมากกว่าการจับผู้กระทำผิดและควรพัฒนากลยุทธ์เพื่อสร้างพื้นที่ปลอดภัยในไซเบอร์สเปสสำหรับการโต้ตอบทางสังคมบนเว็บไซต์เครือข่ายสังคม

ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) (Marcus Felson, Lawrence E. Cohen, 1975) ได้พัฒนาทฤษฎี Routine activity theory อันเกี่ยวเนื่องกับมนุษยนิเวศวิทยา (Human ecology) และทฤษฎีการเลือกอย่างเป็นเหตุเป็นผล (Rational Choice Theory) เห็นว่า อาชญากรรมจะเกิดขึ้นเมื่อมีองค์ประกอบครบ 3 ประการดังภาพประกอบที่ 2.15 ซึ่งมีรายละเอียด ดังนี้

1. เหยื่อ (Victim) หรือเป้าหมาย (Target) หมายถึง บุคคล สถานที่ วัตถุ หรือองค์กรที่อาชญากรรมมุ่งประกอบอาชญากรรมสร้างความเสียหายเพื่อให้ตนได้อรรถประโยชน์
2. โอกาส (Opportunity) หมายถึง ช่วงเวลา (Time) และสถานที่ (Place) ที่เหมาะสม ที่อาชญากรเชื่อว่าสามารถลงมือก่ออาชญากรรมได้หรือเชื่อว่าไม่มีใครจะจับได้
3. อาชญากร (Criminal/Offender) หมายถึง ผู้ที่มีความต้องการ (Crave) จะก่ออาชญากรรมโดยแสวงหาโอกาสตลอดเวลาจากเหยื่อที่อ่อนแอ

หากปัจจัยทั้ง 3 ด้านครบ อาชญากรรมจะเกิดขึ้นทันที ในทางกลับกันหากขาดองค์ประกอบใดอันหนึ่งหายไป อาชญากรรมจะไม่เกิดขึ้น

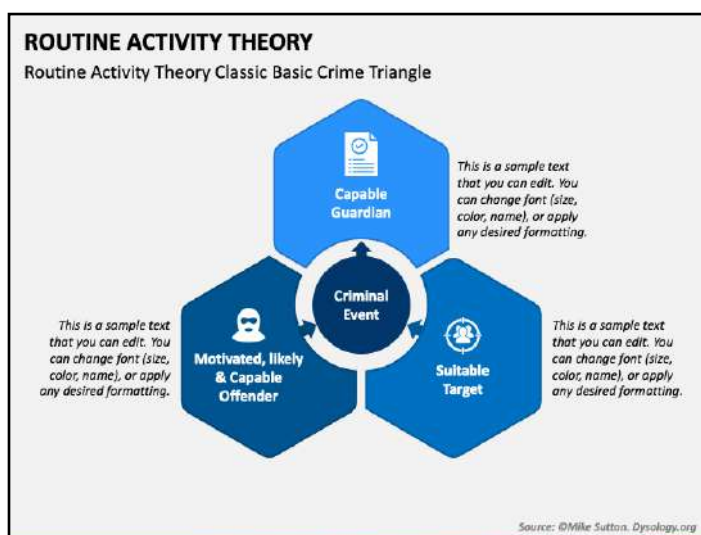


ภาพประกอบที่ 2.15 แสดง Crime Triangle Theory

ที่มา : criminal-justice.iresearchnet.com, 2023

2.4 แนวคิดและทฤษฎีการกระทำที่เป็นกิจวัตรประจำวัน (Theory of Routine Activity)

ทฤษฎีการกระทำที่เป็นกิจวัตรของ (Lawrence E. Cohen และ Marcus Felson, 1979) ที่นำมาอธิบายสาเหตุของโอกาสอาชญากรรม (Crime Opportunity) ซึ่งแนวคิดที่ว่า เรามีกิจวัตรประจำวัน เป็นกิจกรรมที่ทำบ่อยครั้งจนเกิดเป็นความเคยชิน และทำเป็นอย่างสม่ำเสมอ ซึ่งเป็นการให้อาชญากรที่คอยสังเกตการณ์อยู่สามารถประเมิน และวางแผนการกระทำผิด ในสถานการณ์ที่เข้ากันพอดีเรื่องของพื้นที่และเวลา (Space and Time) เมื่อเหยื่อมีพฤติกรรมที่เป็นกิจวัตรประจำวัน เช่น ไปร้านเดิมเป็นประจำ เดินทางไปทำงานเส้นทางที่ไม่ปลอดภัยเป็นประจำ เปิดหน้าต่าง หรือประตูบ้านเป็นวัประจำ ไม่ยอมล็อกประตูหรือหน้าต่างเป็นประจำ ซึ่งโดยองค์ประกอบทั้ง 3 ประการดังภาพประกอบที่ 2.16 ให้เป็นชนวนเหตุทำให้สามารถเกิดอาชญากรรม โดยกล่าวในงานของ (ปรเมศวร์ กุมารบุญ, 2563) ได้แก่



ภาพประกอบที่ 2.16 แสดง Routine Activities Theory

ที่มา : sketchbubble.com, 2023

1. แรงจูงใจอาชญากร (Likely/Motivated offender) อาชญากรมีความปรารถนาหรือความพึงพอใจที่จะหาผลตอบแทนจากเหยื่อได้ตลอดเวลา และอาชญากรมักเห็นโอกาสจากเหยื่อจากการดำเนินกิจวัตรที่มักจูงใจให้ก่ออาชญากรรม และหาประโยชน์จากเหยื่อได้ เมื่อเกิดแรงจูงใจในการก่ออาชญากรรม เช่น เห็นกิจวัตรเหยื่อผ่านสื่อสังคมออนไลน์ไม่ว่าเป็น สถานที่ ภาพถ่าย เวลา หรือช่องว่าง

ของเว็บไซต์หรือระบบคอมพิวเตอร์ขององค์กร ที่อาชญากรมักจะเห็นโอกาสที่สามารถจะบุกรุกเข้าไปได้

2. มีเป้าหมายที่เหมาะสม (Suitable target) อาชญากรจะมองหาเหยื่อที่เป็นเป้าหมายไม่ว่าจะเป็นบุคคลหรือองค์กร ตามที่เหมาะสมกับความสามารถของอาชญากรในการก่ออาชญากรรม เหยื่อก็คือจะมีลักษณะอ่อนแอ มีบุคลิกสับสนเพราะไม่ระมัดระวังตัว เช่น เหยื่อ Romance Scam ที่อาชญากรมักมองหาหญิงที่มีทรัพย์สิน, สูงวัย และขาดประสบการณ์ในการเรียนรู้จักคนจากโลกออนไลน์ ทำให้เชื่อคนง่าย และ ขาดความอบอุ่นหรือขาดความรัก โดยเช่นเดียวกับกลุ่มแฮกเกอร์ใน Darkside มักค้นหาเหยื่อเป้าหมายเพื่อเรียกค่าไถ่ระบบคอมพิวเตอร์ (Ransomware) ซึ่งมักเป็นผู้ใช้งานระบบปฏิบัติการวินโดวส์ที่ไม่ได้มีการปิดช่องโหว่ External Blue

3. ขาดผู้พิทักษ์ที่มีความสามารถ (Lack of a capable guardian) เหยื่อมีความอ่อนแอเป็นปกติทั่วไป จึงต้องมีผู้พิทักษ์ที่คอยสอดส่องดูแลความสงบเรียบร้อย เช่น ตำรวจ ผู้ปกครอง รัฐบาล หรือผู้ดูแลความมั่นคงปลอดภัยไซเบอร์ โอกาสในการเกิดอาชญากรรมจะเกิดขึ้นเมื่อขาดผู้พิทักษ์ที่มีความสามารถเพียงพอในการป้องกันอาชญากรรม

ทฤษฎีกิจกรรมประจำวัน Routine Activities Theory (RAT) ถูกนำมาใช้ในการศึกษาอาชญากรรมไซเบอร์และการตกเป็นเหยื่อทางไซเบอร์ ตามที่ได้กล่าวในงานของ (สาวตรี สุขศรี, 2560 หน้า 427-430) ทฤษฎีชี้ให้เห็นว่า องค์ประกอบข้อ 3 เพราะบุคคลที่มีแนวโน้มของการตกเป็นเหยื่อของอาชญากรรมกลุ่มนี้มากที่สุดคือ ผู้ใช้งานคอมพิวเตอร์ (รวมทั้งอุปกรณ์อิเล็กทรอนิกส์อื่น ๆ ที่เชื่อมต่ออินเทอร์เน็ตได้) ที่ไม่มีมาตรการรักษาความมั่นคงปลอดภัยที่ไม่ทันสมัย (ไม่คอยอัปเดต หรือไม่มีประสิทธิภาพ) หากแต่คือการลดช่องว่างขององค์ประกอบข้อ 3 ด้วยการใช้ระบบรักษาความมั่นคงปลอดภัยดิจิทัล (Digital Guardian) ที่เหมาะสม และเพียงพอ

การศึกษาเหล่านี้เน้นถึงความสำคัญของปัจจัยสถานการณ์และปัจจัยส่วนบุคคลในการทำ ความเข้าใจการตกเป็นเหยื่อทางไซเบอร์ และให้ข้อมูลเชิงลึกสำหรับการพัฒนากลยุทธ์การป้องกันที่มี ประสิทธิภาพ ทฤษฎีกิจกรรมประจำวันสามารถช่วยอธิบายการเพิ่มขึ้นของอาชญากรรมทางไซเบอร์ ในช่วงที่มีกิจกรรมออนไลน์เพิ่มขึ้น เช่น การล็อกดาวน์ทั่วโลกในช่วงการระบาดของ COVID-19

ฐกฤต แก้วทับทิม. (2021) ให้ข้อสรุปไว้ว่า การป้องกันที่ได้ผลมากที่สุด คือ การให้ ความตระหนักรู้ให้แก่ทุกคนในเรื่องความมั่นคงปลอดภัย และป้องกันทางไซเบอร์ โดยแสดงให้เห็น ว่าผู้ที่เป็นเป้าหมายทางอาชญากรรมทางไซเบอร์ มักเป็นบุคคลที่ไม่มีความเข้าใจด้านความเสี่ยง และ ความไม่ปลอดภัยจากการใช้ระบบอินเทอร์เน็ต หากเยาวชน หรือผู้สูงวัย รวมอีกทั้งวัยทำงานที่ขาด

ความรู้ความเข้าใจเกี่ยวกับการใช้ระบบอินเทอร์เน็ตแบบถูกต้อง และปลอดภัย รวมถึงหน่วยงานที่มีการใช้งานระบบข้อมูลส่วนบุคคล และด้านสุขภาพ หรือข้อมูลอ่อนไหว ในช่วงเดียวกับสถานการณ์โรคโควิด-19 เมื่อนำมารวบรวมกับสถานการณ์ที่ขาดความมั่นคงและสับสนของข้อมูลที่พบบนอินเทอร์เน็ตเป็นจำนวนมาก เกิดความไม่เข้าใจเกี่ยวกับโรคระบาดที่ขยายตัวเป็นวงกว้าง และเศรษฐกิจที่ผันผวนกลายเป็นเหตุผลที่ทำให้ผู้ที่ไม่เข้าใจความเสี่ยงด้านไซเบอร์ และบุคคลหรือกลุ่มบุคคล ที่ต้องการหาแนวทางผลประโยชน์จากโรคโควิด-19 ก็ยังทำให้เกิดความเสี่ยงที่มากขึ้นที่จะตกเป็นเหยื่อได้ง่ายจากสถานการณ์นี้ จากภาพประกอบที่ 2.17 แสดงถึงแนวโน้มอาชญากรรมที่เกิดขึ้นระหว่างประเทศ



ภาพประกอบที่ 2.17 แสดงแนวโน้มอาชญากรรมระหว่างประเทศและอาชญากรรมที่เกิดขึ้นใหม่ COVID-19

ที่มา : สถาบันเพื่อการยุติธรรมแห่งประเทศไทย, 2565

ทฤษฎีการกระทำที่เป็นกิจวัตรประจำวัน (Theory of Routine Activity) มีความสามารถในการอธิบายโอกาสในทางทฤษฎีสามเหลี่ยมอาชญากรรมอย่างละเอียดมากขึ้น เน้นไปที่การดำเนินกิจวัตรที่เป็นประจำหรือธรรมชาติของเหยื่อที่มีความอ่อนแอต่อการป้องกันความเสี่ยง ซึ่งสามารถดึงดูด และกระตุ้นให้เกิดอาชญากรรม โดยเฉพาะเมื่อความอ่อนแอของเหยื่อทำให้เกิดความสามารถในการกระทำ

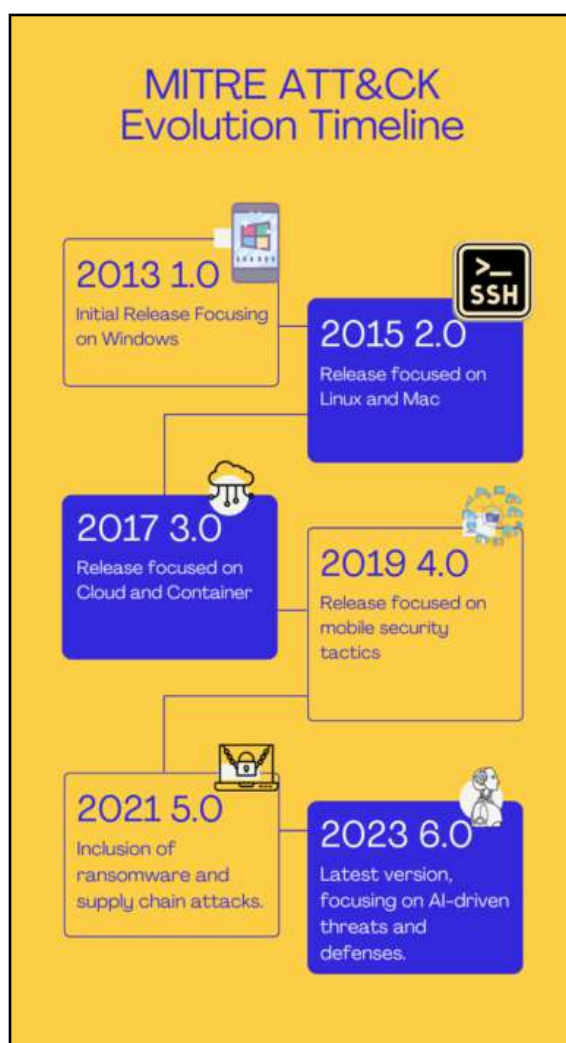
อาชญากรรม ความอ่อนแอที่เสี่ยงต่อความเป็นเหยื่อ รวมกับความอ่อนแอของเหยื่อ อาจไม่ได้รับความสนใจในการปกป้องความมั่นคงปลอดภัยของตนเอง ทำให้มีโอกาที่ผู้กระทำอาชญากรรมจะมองเห็นโอกาส และลองกระทำอาชญากรรมขึ้น ทั้งนี้ เพื่อดำเนินการในกระบวนการทางทฤษฎีสามเหลี่ยมอาชญากรรมอย่างมีประสิทธิภาพ ควรมีผู้ที่สามารถดูแลหรือผู้พิทักษ์ ทั้งภายในครอบครัว องค์กร และสังคม เพื่อเสริมสร้างการป้องกัน และรักษาความมั่นคงปลอดภัยของเหยื่อให้มากยิ่งขึ้น นอกจากนี้ การให้ความรู้และการสร้างความตระหนักในความเสี่ยงที่อาจเกิดขึ้นก็เป็นสิ่งสำคัญในกระบวนการนี้ด้วย การควบคุมโอกาสและรับผิดชอบต่อความมั่นคงปลอดภัยสามารถช่วยลดความเสี่ยงในการเกิดอาชญากรรมทางไซเบอร์และอาชญากรรมอื่น ๆ อย่างมีประสิทธิภาพได้อย่างมาก

2.5 หลักการเกี่ยวกับ MITRE ATT&CK Framework

หลักการของ MITRE ATT&CK เป็นแบบจำลองการจำแนกประเภทการโจมตีที่ครอบคลุมซึ่งจัดหมวดหมู่กลยุทธ์ เทคนิค และขั้นตอนของผู้โจมตีไซเบอร์อย่างเป็นระบบได้รับการนำมาใช้กันอย่างแพร่หลายโดยอุตสาหกรรมความมั่นคงปลอดภัยทางไซเบอร์ และนักวิจัยทางวิชาการสำหรับการใช้งานต่าง ๆ เช่นข่าวกรองภัยคุกคามการตรวจจับภัยคุกคาม และการตอบสนองต่อเหตุการณ์ กรอบการทำงานนี้ให้ฐานความรู้เกี่ยวกับกลยุทธ์ และเทคนิคของฝ่ายตรงข้าม ทำให้องค์กรสามารถวิเคราะห์ และปรับปรุงกลไกการรับรองความถูกต้องเพื่อป้องกันช่องโหว่ที่อาจเกิดขึ้นและการเข้าถึงโดยไม่ได้รับอนุญาต ด้วยการใช้ MITRE ATT&CK บริษัทต่าง ๆ สามารถระบุและแก้ไขจุดอ่อนในระบบการรับรองความถูกต้อง ตลอดจนพัฒนามาตรการที่มีประสิทธิภาพสำหรับการตรวจจับ ป้องกัน และการบรรเทาการโจมตีที่อาจเกิดขึ้น ประโยชน์ของกรอบในการใช้งานที่แตกต่างกันได้รับการศึกษา และมีความจำเป็นต้องมีการวิจัยเพิ่มเติมเกี่ยวกับการนำไปใช้ และการประเมินในทางปฏิบัติ เนื่องจาก MITRE ATT&CK เป็นเครื่องมือที่มีประสิทธิภาพในการช่วยให้องค์กรเข้าใจและเตรียมการตรวจจับและป้องกันการโจมตีทางไซเบอร์ในลักษณะที่เป็นไปได้มากขึ้น และการวิจัยเพิ่มเติมจะช่วยให้ผู้ใช้ในอุตสาหกรรมความมั่นคงปลอดภัยทางไซเบอร์พัฒนากลยุทธ์การป้องกันและปรับปรุงความมั่นคงปลอดภัยอย่างมีประสิทธิภาพในเวลาจริง รวมถึงการใช้เทคโนโลยีที่ทันสมัยในการตรวจจับ และป้องกันการโจมตีทางไซเบอร์ที่กำลังเกิดขึ้นในระบบของพวกเขา

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) ที่ถูกพัฒนาโดย MITRE Corporation ซึ่งเป็นองค์กรไม่แสวงผลกำไรในสหรัฐอเมริกาที่มุ่งเน้นการวิจัย และพัฒนาทางเทคโนโลยี โครงการ MITRE ATT&CK เริ่มต้นขึ้นเพื่อช่วยองค์กรป้องกันการโจมตีทางไซเบอร์ให้มี

ความเข้าใจและการเรียนรู้ในระดับเชิงลึกเกี่ยวกับวิธีการที่ผู้โจมตีเพื่อเข้าถึงระบบ และข้อมูลขององค์กร โครงการนี้เริ่มต้นในปี 2013 (Michael Toback, 2023) และมีการอัปเดตและพัฒนาต่อเนื่องจนถึงปัจจุบัน จากรายละเอียดที่แสดงดังภาพประกอบที่ 2.18



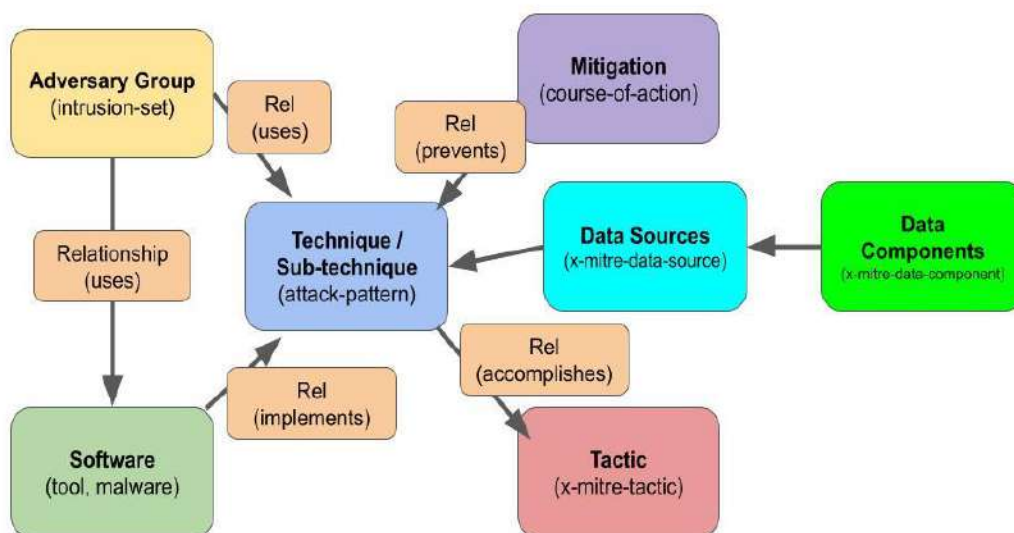
ภาพประกอบที่ 2.18 แสดง Evolution of MITRE ATT&CK Timeline

ที่มา : Smallbizepp.com, 2023

MITRE ATT&CK มุ่งเน้นให้ความรู้และข้อมูลที่เกี่ยวข้องกับวิธีการของผู้โจมตีเป็นสิ่งสำคัญ โดยจำแนกแยกประเภทการโจมตีออกเป็นกลยุทธ์ (Tactics) เทคนิค (Techniques) และขั้นตอน (Procedures)

ที่สามารถใช้เพื่อทำให้การโจมตีสำเร็จ การจำแนกนี้ช่วยให้องค์กรสามารถทำความเข้าใจการทำงานของผู้โจมตีไซเบอร์ใช้ความรู้นี้ในการป้องกัน และตรวจจับการโจมตี

MITRE ATT&CK เปิดให้สาธารณชนเข้าถึงและใช้งานได้ฟรี และมีคอมมูนิตีที่ใช้ร่วมกันเพื่อพัฒนาและอัปเดตข้อมูลเกี่ยวกับการโจมตี โครงการนี้มีความสำคัญในการเสริมสร้างความเข้าใจและความรู้ในสาขาความมั่นคงปลอดภัยทางไซเบอร์ และช่วยองค์กรในการพัฒนากลยุทธ์การป้องกันที่มีประสิทธิภาพต่อการโจมตีทางไซเบอร์ที่เปลี่ยนแปลงอยู่เสมอ ดังภาพประกอบที่ 2.19



ภาพประกอบที่ 2.19 แสดง ATT&CK Objects are modelled

ที่มา : signalcorps.com, 2022

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) เป็นโครงข่ายทางไซเบอร์ที่มีความหมายอย่างลึกซึ้งสำหรับการจำแนกประเภทการโจมตีทางไซเบอร์เราจะพิจารณา Core Components เวอร์ชัน 13.1 ที่เริ่มใช้งานตั้งแต่ 25 เมษายน 2566 หรือส่วนประจําของ MITRE ATT&CK อย่างละเอียดดังนี้ (<https://attack.mitre.org>, 2023)

Tactics (กลยุทธ์) กลยุทธ์ใน MITRE ATT&CK คือหลักของการดำเนินการทางไซเบอร์ที่ผู้โจมตีใช้เพื่อเป้าหมายหลัก เช่นการเข้าถึงระบบหรือการขโมยข้อมูล มี 14 กลยุทธ์ ที่ครอบคลุมหลายด้านของ

การโจมตีได้แก่ Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection Command and Control, Exfiltration และ Impact ซึ่งแสดงรายละเอียดตามภาพประกอบที่ 2.20

Enterprise tactics		
Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.		
Enterprise Tactics: 14		
ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

ภาพประกอบที่ 2.20 แสดง MITRE ATT&CK TACTICS: ENTERPRISE

ที่มา : attack.mitre.org, 2023

1. Reconnaissance (การลาดตระเวน) กลยุทธ์ที่เน้นในขั้นตอนการสืบหาข้อมูลและรับรู้เกี่ยวกับระบบและเป้าหมายของผู้โจมตี โดยไม่ทำลายข้อมูลหรือทรัพยากรของเป้าหมาย ฟังก์ชันหลักของกลยุทธ์ Reconnaissance คือการเข้าถึงข้อมูลเข้าหน้าที่บุคลากรของเหยื่อ หรือสิ่งของที่อยู่ในระบบหรือองค์กรเป้าหมายเพื่อเตรียมการสำหรับการโจมตีต่อไป รวมถึงการรวบรวมข้อมูลเกี่ยวกับโครงสร้างของระบบ ช่องโหว่ที่อาจใช้ประโยชน์ได้ ข้อมูลผู้ใช้ และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับเป้าหมาย

2. Resource Development (การพัฒนาทรัพยากร) เป็นเทคนิคที่ใช้เพื่อสร้างหรือเพิ่มเติมทรัพยากรที่จำเป็นสำหรับการโจมตี สามารถใช้เพื่อสนับสนุนการกำหนดเป้าหมายได้ ทรัพยากรดังกล่าวรวมถึงโครงสร้างพื้นฐาน บัญชี หรือความสามารถของฝ่ายตรงข้าม ที่สามารถใช้ประโยชน์จากทรัพยากรเหล่านี้ ทรัพยากรที่อาจจะรวมถึงเครื่องมือ การโปรแกรม และข้อมูลที่สามารถใช้ในการโจมตีอย่างมีประสิทธิภาพ

3. Initial Access (การเข้าถึงเบื้องต้น) เทคนิคที่ใช้เวกเตอร์รายการต่าง ๆ เพื่อตั้งหลักเริ่มต้น เทคนิคที่ใช้ได้แก่ การกำหนดเป้าหมายแบบ Spear-Phishing และการใช้ประโยชน์จากจุดอ่อนบน Web Server ที่เปิดเผยต่อสาธารณะ การเข้าถึงครั้งแรกอาจอนุญาตให้เข้าถึงได้อย่างต่อเนื่อง เช่น บัญชีที่ถูกดักและการใช้บริการระยะไกลภายนอก หรืออาจถูกจำกัดการใช้งานเนื่องจากการเปลี่ยนรหัสผ่าน หลักการ Initial Access จะเป็นขั้นตอนแรกในลำดับการดำเนินการโจมตีไซเบอร์ที่ผู้โจมตีดำเนินการ โดยใช้หลายเทคนิคและเครื่องมือต่าง ๆ เช่นการสแกนเครือข่าย การใช้ช่องโหว่ที่มีอยู่ การสร้าง หรือนำเข้าเครื่องมือสำหรับการโจมตี (Exploits) การเรียกดูหรือร้องขอเข้าถึงข้อมูลข่าวสารสำคัญ หรือการสร้างทรัพยากรที่จำเป็นสำหรับการโจมตี (Resource Development) อย่างมีประสิทธิภาพ

4. Execution (การดำเนินการ) เทคนิคและเครื่องมือต่าง ๆ หรือชุดคำสั่งเพื่อดำเนินการโจมตีได้ อย่างไรก็ตามมันอาจไม่จำเป็นต้องอยู่ในรูปแบบของการประมวลผลโปรแกรมเท่านั้น มีหลายวิธีที่ผู้โจมตีสามารถใช้เพื่อทำการ Execution อย่างมีประสิทธิภาพเช่น การรันสคริปต์ การใช้ช่องโหว่ การโหลดแพลตฟอร์มที่ไม่ได้รับอนุญาต หรือการรันโปรแกรมที่มีฟังก์ชันแบ็กโดอร์ (Backdoor) เพื่อเปิดทางให้ผู้โจมตีเข้าถึงระบบให้มีความควบคุม

5. Persistence (การคงอยู่) เทคนิคที่ฝ่ายตรงข้ามใช้เพื่อรักษาการเข้าถึงระบบระหว่างการรีสตาร์ท การเปลี่ยนแปลงข้อมูลประจำตัว และการหยุดชะงักอื่น ๆ ที่อาจตัดการเข้าถึงของพวกเขา เทคนิคที่ใช้เพื่อความคงอยู่ ได้แก่ การเข้าถึง การดำเนินการ หรือการเปลี่ยนแปลงการกำหนดค่าที่ช่วยให้สามารถรักษาคูณบนระบบได้ เช่น การเปลี่ยน หรือ Hijacking โค้ดที่ถูกต้อง หรือการเพิ่มโค้ดเริ่มต้น

6. Privilege Escalation (การเพิ่มสิทธิ์) เทคนิคที่ฝ่ายตรงข้ามใช้เพื่อรับสิทธิ์ระดับที่สูงกว่าบนระบบหรือเครือข่าย ฝ่ายตรงข้ามมักจะสามารถเข้าและสำรวจเครือข่ายที่มีการเข้าถึงที่ไม่มีสิทธิ์พิเศษ แต่ต้องได้รับการอนุญาตระดับสูงเพื่อปฏิบัติตามวัตถุประสงค์ของพวกเขา แนวทางทั่วไปคือการใช้ประโยชน์จากจุดอ่อนของระบบ การกำหนดค่าที่ไม่ถูกต้อง และช่องโหว่ ตัวอย่างของการเข้าถึงแบบยกระดับ ได้แก่ ระบบระดับราก ผู้ดูแลระบบ บัญชีผู้ใช้ที่มีสิทธิ์การเข้าถึงเหมือนผู้ดูแลระบบ และบัญชี

ผู้ใช้ที่สามารถเข้าถึงระบบเฉพาะหรือทำหน้าที่เฉพาะได้ ซึ่งเทคนิคเหล่านี้มักจะทับซ้อนกับเทคนิค Persistence เนื่องจากคุณสมบัติของระบบปฏิบัติการที่ถูกโจมตียังคงอยู่และสามารถดำเนินการได้ในบริบทที่มีการยกระดับ

7. Defense Evasion (การหลบหลีกการป้องกัน) เทคนิคที่ผู้โจมตีใช้เพื่อหลีกเลี่ยงหรือทำให้มาตรการป้องกันทางไซเบอร์ที่ถูกติดตั้งในระบบ หรือโครงข่ายของเป้าหมายไม่สามารถตรวจจับหรือป้องกันการโจมตีได้ คุณลักษณะนี้ช่วยให้ผู้โจมตีสามารถดำเนินการโจมตีได้อย่างไม่รู้ตัวหรือให้มาตรการป้องกันทางไซเบอร์ไม่สามารถป้องกันการโจมตีได้อย่างมีประสิทธิภาพ และ Defense Evasion มีอีกหลายวิธี ที่ผู้โจมตีสามารถใช้ เช่น การเข้ารหัสข้อมูล การเปลี่ยนชื่อแฟ้มหรือหน้าจอ การเปิดใช้ช่องโหว่ที่ยังไม่มีการรับรองความถูกต้อง (Zero-Day Vulnerabilities), ปิดการใช้งานซอฟต์แวร์ ความมั่นคงปลอดภัย การปลอมแปลงข้อมูลการรับรองความถูกต้อง (Spoofing) และการแก้ไขลำดับช่องโหว่ที่มีอยู่ เพื่อหลีกเลี่ยงการตรวจจับหรือการป้องกันการตรวจพบการโจมตี

8. Credential Access (การเข้าถึงข้อมูลประจำตัว) เทคนิคในการขโมยข้อมูลประจำตัว เช่น ชื่อ บัญชีและรหัสผ่าน เทคนิคที่ใช้ในการรับข้อมูลรับรอง ได้แก่ การล่อลวงหรือการทวงข้อมูลรับรอง การใช้ข้อมูลประจำตัวที่ถูกต้องตามกฎหมายสามารถให้ฝ่ายตรงข้ามเข้าถึงระบบ ทำให้ตรวจพบได้ยากขึ้น และให้โอกาสในการสร้างบัญชีเพิ่มเติมเพื่อช่วยให้บรรลุเป้าหมาย

9. Discovery (การค้นพบ) เทคนิคหรือขั้นตอนที่ผู้โจมตีใช้เพื่อสำรวจหรือค้นหาข้อมูลเกี่ยวกับระบบหรือโครงข่ายของเป้าหมาย การ Discovery ช่วยให้ผู้โจมตีได้ข้อมูลที่จำเป็นเพื่อการวางแผนและดำเนินการโจมตีอย่างมีประสิทธิภาพ และสามารถใช้เทคนิคและเครื่องมือต่าง ๆ เพื่อค้นหาข้อมูลที่อยู่ในระบบหรือโครงข่าย เช่น การสแกนเครือข่าย การค้นหาข้อมูลในระบบไฟล์ หรือการสืบค้นทรัพยากรในเครือข่าย นอกจากนี้อาจเกี่ยวข้องกับการสอบถามหรือพยากรณ์เพื่อค้นหาข้อมูลเชิงลึกหรือข้อมูลที่เป็นประโยชน์สำหรับการโจมตี

10. Lateral Movement (การเคลื่อนไหวย้ายข้าง) เทคนิคที่ฝ่ายตรงข้ามใช้ในการเข้า และควบคุมระบบระยะไกลบนเครือข่าย การทำตามวัตถุประสงค์หลักมักจะต้องมีการสำรวจเครือข่ายเพื่อค้นหาเป้าหมาย และเข้าถึงเครือข่ายนั้นในภายหลัง การบรรลุวัตถุประสงค์มักเกี่ยวข้องกับการหมุนเวียนผ่านระบบ และบัญชีต่าง ๆ เพื่อให้ได้มาซึ่ง ฝ่ายตรงข้ามอาจติดตั้งเครื่องมือการเข้าถึงระยะไกลของตนเอง เพื่อให้การเคลื่อนไหวย้ายข้างสำเร็จ หรือใช้ข้อมูลประจำตัวที่ถูกต้องกับเครือข่ายดั้งเดิม และเครื่องมือระบบปฏิบัติการ ซึ่งอาจเป็นความลับมากกว่า

11. Collection (การรวบรวมข้อมูล) เทคนิคที่ฝ่ายตรงข้ามอาจใช้เพื่อรวบรวมข้อมูลและข้อมูลแหล่งที่มาจะถูกรวบรวมจากที่เกี่ยวข้องกับการติดตามวัตถุประสงค์ของฝ่ายตรงข้าม บ่อยครั้ง เป้าหมายต่อไปหลังจากการรวบรวมข้อมูลคือการขโมย (กรอง) ข้อมูล แหล่งที่มาเป้าหมายทั่วไป ได้แก่ ใครฟี่ประเภทต่าง ๆ เบราวเซอร์ เสียง วิดีโอ และอีเมล วิธีการเก็บรวบรวมทั่วไป ได้แก่ การจับภาพหน้าจอและการป้อนข้อมูลด้วยแป้นพิมพ์

12. Command and Control (คำสั่งและการควบคุม) เทคนิคที่ฝ่ายตรงข้ามอาจใช้เพื่อสื่อสารกับระบบภายใต้การควบคุมภายในเครือข่ายของเหยื่อ โดยทั่วไปแล้วฝ่ายตรงข้ามจะพยายามเลียนแบบการรับส่งข้อมูลปกติที่คาดหวังเพื่อหลีกเลี่ยงการตรวจจับ มีหลายวิธีที่ฝ่ายตรงข้ามสามารถสร้างคำสั่งและการควบคุมด้วยการซ่อนตัวในระดับต่างๆ ขึ้นอยู่กับโครงสร้างเครือข่าย และการป้องกันของเหยื่อ

13. Exfiltration (การคัดกรอง) เทคนิคที่ฝ่ายตรงข้ามอาจใช้เพื่อขโมยข้อมูลจากเครือข่ายของคุณ เมื่อพวกเขารวบรวมข้อมูลแล้ว ฝ่ายตรงข้ามมักจะจัดแพ็คเกจเพื่อหลีกเลี่ยงการตรวจจับขณะลบออก ซึ่งอาจรวมถึงการบีบอัดและการเข้ารหัส เทคนิคในการดึงข้อมูลออกจากเครือข่ายเป้าหมายโดยทั่วไปจะรวมถึงการถ่ายโอนข้อมูลผ่านช่องทางคำสั่ง และการควบคุมหรือช่องทางอื่น และอาจรวมถึงการจำกัดขนาดในการส่งข้อมูลด้วย

14. Impact (ผลกระทบ) เทคนิคที่ฝ่ายตรงข้ามใช้เพื่อขัดขวางความพร้อมใช้งานหรือประนีประนอมความสมบูรณ์โดยการจัดการทางธุรกิจ และกระบวนการปฏิบัติงาน เทคนิคที่ใช้ในการส่งผลกระทบอาจรวมถึงการทำลายหรือแก้ไขข้อมูล ในบางกรณี กระบวนการทางธุรกิจอาจดูดี แต่อาจมีการเปลี่ยนแปลงเพื่อให้เป็นประโยชน์ต่อเป้าหมายของฝ่ายตรงข้าม ฝ่ายตรงข้ามอาจใช้เทคนิคเหล่านี้เพื่อปฏิบัติตามเป้าหมายสุดท้ายหรือเพื่อปิดกั้นการละเมิดการรักษาความลับ

Techniques (เทคนิค) คือขั้นตอนและวิธีการที่ผู้โจมตีใช้เพื่อดำเนินการในขั้นตอนแต่ละของกลยุทธ์ มีรายการของเทคนิคในแต่ละกลยุทธ์ที่อธิบายวิธีการทำในระดับที่เฉพาะเจาะจง ซึ่งช่วยให้องค์กรรู้จักวิธีการที่สามารถถูกใช้ในการโจมตี มีเทคนิคหลายร้อยวิธีที่ถูกนำมาอธิบายใน MITRE ATT&CK แต่ละกลยุทธ์มีเทคนิคที่เกี่ยวข้องอธิบายวิธีจากการโจมตีทางไซเบอร์ 5 เทคนิคของ MITRE ATT&CK ที่รายงานที่ถูกนำมาใช้มากที่สุด ดังภาพประกอบที่ 2.21 (Log point Top 10 Critical MITRE ATT&CK Techniques, 2022) คือ

1. T1059 Command and Scripting Interpreter เป็นการโจมตีโดยใช้ตัวแปลคำสั่งและสคริปต์ในทางที่ผิดเพื่อดำเนินการคำสั่ง สคริปต์ หรือไบนารี อินเทอร์เฟซ และภาษาเหล่านี้ให้วิธีการโต้ตอบกับระบบคอมพิวเตอร์ และเป็นคุณลักษณะทั่วไปในแพลตฟอร์มต่างๆ มากมาย ระบบส่วนใหญ่มา

พร้อมกับอินเทอร์เน็ตเบราว์เซอร์ที่คำสั่ง และความสามารถในการเขียนสคริปต์ในตัว ตัวอย่างเช่น ระบบปฏิบัติการ macOS และ Linux จะมีระบบปฏิบัติการ Unix Shell อยู่บ้าง ในขณะที่การติดตั้ง Windows จะมี Windows Command Shell และ PowerShell อยู่ด้วย

2. T1003 OS Credential Dumping เป็นการโจมตีโดยพยายามถ่ายโอนข้อมูลประจำตัวเพื่อรับการเข้าสู่ระบบบัญชี และเอกสารรับรอง โดยปกติจะอยู่ในรูปแบบของแฮชหรือรหัสผ่านข้อความที่ชัดเจนจากระบบปฏิบัติการและซอฟต์แวร์ ข้อมูลรับรองสามารถใช้เพื่อดำเนินการเคลื่อนไหวด้านข้างและเข้าถึงข้อมูลที่จำกัดได้

3. T1090 Proxy เป็นการโจมตีใช้พร็อกซีการเชื่อมต่อเพื่อกำหนดเส้นทางการรับส่งข้อมูลเครือข่ายระหว่างระบบ หรือทำหน้าที่เป็นตัวกลางสำหรับการสื่อสารเครือข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่ายคำสั่ง และควบคุมเพื่อหลีกเลี่ยงการเชื่อมต่อโดยตรงกับโครงสร้างพื้นฐานของพวกเขา มีเครื่องมือมากมายที่เปิดใช้งานการเปลี่ยนเส้นทางการรับส่งข้อมูลผ่านพร็อกซีหรือการเปลี่ยนเส้นทางพอร์ต รวมถึง HTRAN, ZXProxy และ ZXPortMap ผู้โจมตีใช้พร็อกซีประเภทนี้เพื่อจัดการคำสั่งและการควบคุมการสื่อสาร ลดจำนวนการเชื่อมต่อเครือข่ายขาออกพร้อมกัน ให้ความยืดหยุ่นเมื่อเผชิญกับการสูญเสียการเชื่อมต่อ หรือเพื่อข้ามเส้นทางสื่อสารที่เชื่อถือได้ที่มีอยู่ระหว่างเหยื่อเพื่อหลีกเลี่ยงความสงสัย ผู้โจมตีอาจเชื่อมโยงพร็อกซีหลายตัวเข้าด้วยกันเพื่อปิดบังแหล่งที่มาของการรับส่งข้อมูลที่เป็นอันตราย

4. T1055 Process Injection ผู้โจมตีแทรกโค้ดเข้าไปในกระบวนการเพื่อหลีกเลี่ยงการป้องกันตามกระบวนการ และอาจยกระดับสิทธิพิเศษด้วย การแทรกกระบวนการเป็นวิธีการรันโค้ดตามอำเภอใจในพื้นที่ที่อยู่ของกระบวนการสดที่แยกจากกัน การรันโค้ดในบริบทของกระบวนการอื่นอาจทำให้สามารถเข้าถึงหน่วยความจำของกระบวนการ ทรัพยากรระบบเครือข่าย และอาจมีสิทธิ์การยกระดับ การดำเนินการผ่านการฉีดกระบวนการอาจหลบเลี่ยงการตรวจจับจากผลิตภัณฑ์รักษาความมั่นคงปลอดภัย เนื่องจากการดำเนินการถูกปิดกั้นภายใต้กระบวนการที่ต้องตามกฎหมาย

5. T1036 Masquerading ผู้โจมตีพยายามจัดการคุณลักษณะของตนเพื่อให้ปรากฏว่าถูกต้องหรือไม่เป็นพิษเป็นภัยต่อผู้ใช้และ/หรือเครื่องมือรักษาความมั่นคงปลอดภัย การปลอมตัวเกิดขึ้นเมื่อชื่อหรือที่ตั้งของวัตถุ ไม่ว่าจะถูกต้องตามกฎหมายหรือเป็นอันตราย ถูกบงการหรือใช้ในทางที่ผิดเพื่อหลบเลี่ยงการป้องกัน และการสังเกต ซึ่งอาจรวมถึงการจัดการข้อมูลเมตาของไฟล์ การหลอกผู้ใช้ให้ระบุประเภทไฟล์ผิด และการให้ชื่องาน หรือบริการที่ต้องการ

Data Sources (แหล่งข้อมูล) แหล่งข้อมูลที่สามารถใช้ในการตรวจสอบการโจมตี เช่น บันทึกการเข้าถึงระบบ (Logs) และข้อมูลการเคลื่อนที่ของข้อมูล ดังภาพประกอบที่ 2.21



ภาพประกอบที่ 2.21 แสดง Log point Top 10 Critical MITRE ATT&CK Techniques
ที่มา : logpoint.com, 2022

Mitigations (มาตรการป้องกัน) ระบุมาตรการที่องค์กรสามารถนำมาใช้เพื่อลดความเสี่ยงที่เกี่ยวข้องกับเทคนิคและขั้นตอนต่าง ๆ ใน MITRE ATT&CK นี้รวมถึงมาตรการที่องค์กรสามารถนำมาใช้เพื่อป้องกันการโจมตีหรือลดความเสี่ยง เช่น การปิดพอร์ตที่ไม่จำเป็นหรือการใช้การตรวจสอบความถูกต้องสำหรับการเข้าถึงบัญชีผู้ใช้เพื่อลดความเสี่ยงในการโจมตี และรักษาความมั่นคงปลอดภัยของระบบข้อมูลขององค์กรของคุณไว้ในระดับสูงสุด

Groups (กลุ่ม) หมายถึงกลุ่มหรือองค์กรหรือกลุ่มบุคคลที่มีกิจกรรมการโจมตีทางไซเบอร์ และถูกติดตาม หรือเก็บข้อมูลโดยชื่อรวมในชุมชนด้านความมั่นคงปลอดภัย นักวิเคราะห์แต่ละคนติดตามกลุ่มเหล่านี้โดยใช้วิธีการวิเคราะห์ต่าง ๆ และอาจใช้คำที่แตกต่างกันเรียกกลุ่มเหล่านี้ เช่น กลุ่มความเสี่ยง

กลุ่มกิจกรรมหรือนักเรียน นักวิเคราะห์อาจติดตามกลุ่มเหล่านี้โดยใช้เทคนิคการวิเคราะห์ต่าง ๆ และคำว่ากลุ่มความเสี่ยง กลุ่มกิจกรรม หรือนักเรียน

Software (ซอฟต์แวร์) หมายถึง ซอฟต์แวร์หรือโปรแกรมคอมพิวเตอร์ที่ผู้โจมตีใช้เพื่อดำเนินการโจมตีหรือเข้าถึงระบบหรือโครงข่ายของเป้าหมาย ซอฟต์แวร์นี้อาจมีหลายประเภท และใช้เพื่อวัตถุประสงค์แตกต่าง ๆ ขึ้นอยู่กับลักษณะของการโจมตีและเป้าหมายของผู้โจมตี MITRE ATT&CK อาจมาจากหลายแหล่งที่ผู้โจมตีนำมาใช้หรือสร้างขึ้นเอง ซอฟต์แวร์นี้มักถูกใช้เพื่อทำ Execution หรือดำเนินการโจมตีทางไซเบอร์อื่น ๆ ได้ เช่น Malware (มัลแวร์), Exploits (โปรแกรมที่ใช้ช่องโหว่), RATs (Remote Access Trojans) และ Backdoors (โปรแกรมที่ทำให้ผู้โจมตีสามารถเข้าถึงระบบได้โดยไม่รู้ตัว)

Procedures (ขั้นตอน) ลักษณะของการดำเนินการของผู้โจมตี รวมถึงขั้นตอนที่ต้องสามารถทำได้เพื่อเริ่มการโจมตี และขั้นตอนที่ต้องทำหลังจากการ Initial Access และ Execution หรือการเข้าถึงและการดำเนินการต่อไป เช่น ขั้นตอนในการโจมตีอาจรวมการเรียกใช้โปรแกรมบนเครือข่าย การสร้างช่องโหว่ในระบบ การนำเข้าโปรแกรมลับหรืออื่น ๆ การพยายามเข้าถึงข้อมูลข่าวสารอย่างบางอย่าง การค้นหาข้อมูลหรือการดำเนินการอื่น ๆ ที่เกี่ยวข้องกัวัตถุประสงค์หรือเป้าหมายของการโจมตี

MITRE ATT&CK เป็นแบบจำลองทางไซเบอร์ที่รายละเอียด และเป็นที่ยอมรับอย่างแพร่หลายในสาขาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งช่วยให้องค์กร และนักวิจัยสามารถทำความเข้าใจ และวิเคราะห์การโจมตีได้อย่างมีประสิทธิภาพ โดยสรุปเกี่ยวกับ MITRE ATT&CK ไว้ดังนี้

1. MITRE ATT&CK เป็นแบบจำลองทางไซเบอร์ ที่อธิบายกลยุทธ์ และเทคนิคที่ผู้โจมตีใช้เพื่อดำเนินการโจมตีในระบบหรือโครงข่ายของเป้าหมาย มี 14 กลยุทธ์ และหลายร้อยเทคนิคที่สามารถใช้ในการโจมตี

2. สำหรับการอบรมและการป้องกัน MITRE ATT&CK เป็นทรัพยากรที่มีประโยชน์สำหรับการอบรมนักวิจัย และผู้ปฏิบัติการด้านความมั่นคงปลอดภัย ช่วยให้องค์กรสามารถเพิ่มความระมัดระวัง และการเตรียมความพร้อมในการตรวจจับ และป้องกันการโจมตีทางไซเบอร์

3. ป้องกันและตรวจจับ MITRE ATT&CK ช่วยให้องค์กรสามารถรู้จัก และเข้าใจแนวทางการโจมตีทางไซเบอร์ และนำมาตรการที่เหมาะสมสำหรับป้องกัน และตรวจจับการโจมตีที่อาจเกิดขึ้นในระบบของพวกเขา หรือปรับปรุงระบบตรวจจับให้มีความเข้าใจการโจมตีให้มากขึ้น และทันต่อปัจจุบัน

4. นำไปใช้ในการวิจัย MITRE ATT&CK เป็นทรัพยากรที่นักวิจัยสามารถใช้ในการศึกษาแนวคิดในการโจมตีทางไซเบอร์และสำหรับการพัฒนามาตรระบบการในการป้องกัน และตรวจจับการโจมตีได้แม่นยำมากขึ้น

5. ระบบป้องกันที่รองรับการทำงานร่วมกัน MITRE ATT&CK ช่วยสนับสนุนความร่วมมือระหว่างองค์กร และนักวิจัยทางความมั่นคงปลอดภัยในการเข้าใจ และตอบสนองต่อการโจมตีทางไซเบอร์ในระบบของพวกเขา

โดยสรุป MITRE ATT&CK เป็นเครื่องมือที่มีประสิทธิภาพในการเพิ่มความระมัดระวังและความเข้าใจในการโจมตีทางไซเบอร์ และช่วยให้องค์กรสามารถป้องกัน และตรวจจับการโจมตีได้อย่างมีประสิทธิภาพ

2.6 หลักการเกี่ยวกับระบบ Security Information & Event Management (SIEM)

หากเราต้องการที่รวบรวมการเฝ้าระวังความผิดปกติหรือภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพของระบบการตรวจจับ และวิเคราะห์เหตุการณ์ เพื่อให้สามารถตรวจจับกิจกรรม ที่ไม่พึงประสงค์หรือเป็นอันตรายต่อระบบได้อย่างทันเหตุการณ์ ในปัจจุบันคงต้องหันไม่พ้นระบบ SIEM ซึ่งถูกใช้กันอย่างแพร่หลายในปัจจุบัน ซึ่งตามที่ (พรบ การรักษาความมั่นคงปลอดภัยไซเบอร์, 2562) ได้มีการระบุเป็นสำคัญว่า

หน่วยงานที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางด้านการสารสนเทศ ต้องกำหนดให้มีแนวทางการจัดระบบหรือขั้นตอนที่เกี่ยวข้องในการเฝ้าระวังความเสี่ยงทางไซเบอร์ และเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ของโครงสร้างพื้นฐานสารสนเทศสำคัญของตน เป็นไปตามมาตรฐานที่ถูกกำหนดโดยหน่วยงานควบคุมที่กำกับดูแลปฏิบัติตามแนวทางปฏิบัติที่ระบุ จึงทำให้มีความจำเป็นอย่างมากในการจัดตั้งศูนย์ระวังภัย ทางไซเบอร์ประกอบกับต้องจัดหาอุปกรณ์หรือเทคโนโลยี เพื่อช่วยดำเนินการเรื่องความมั่นคงปลอดภัยด้านไซเบอร์ เพื่อสอดคล้องกับข้อบังคับตามที่ (พรบ การรักษาความมั่นคงปลอดภัยไซเบอร์, 2562) ที่กล่าวมาข้างต้น

2.6.1 จุดเริ่มต้นของระบบ Security Information & Event Management (SIEM)

จากงานเขียนของ (Vlad-Mihai Cotenescu, 2017) ระบบ SIEM มีมาตั้งแต่ปี ค.ศ 2000 และมีการพัฒนาอย่างต่อเนื่องเพื่อติดตามการเปลี่ยนแปลงอย่างรวดเร็วในสภาพแวดล้อมที่ใช้เทคโนโลยี SIEM รวมการจัดการข้อมูลความมั่นคงปลอดภัย (SIM) และการจัดการเหตุการณ์ความมั่นคงปลอดภัย (SEM) เพื่อให้การวิเคราะห์การแจ้งเตือนความมั่นคงปลอดภัยแบบเรียลไทม์ ด้วย Log จากที่เกิดขึ้นโดย

ระบบปฏิบัติการบนอุปกรณ์หรือ Log ของแอปพลิเคชันนั้นๆ ด้วยหลักการนี้ SIEM จะทำการรวบรวมและวิเคราะห์ข้อมูลทั้งหมดที่เกี่ยวข้องเกี่ยวกับความมั่นคงปลอดภัย ซึ่งช่วยให้สามารถระบุแนวโน้มที่น่าจะเป็น และรูปแบบต่างๆที่ไม่เป็นปกติได้ง่ายขึ้น ระบบ SIEM เป็นการลงทุนที่มีความสำคัญมาก สำหรับองค์กรที่ต้องการความมั่นคงปลอดภัยของระบบที่มีคุณภาพสูง และสามารถตอบสนองต่อภัยคุกคามได้อย่างถูกต้อง และปรับลดความเสี่ยงของระบบสารสนเทศ และการปฏิบัติงานของผู้ดูแลระบบ อย่างไรก็ตาม SIEM ถือเป็นระบบที่ซับซ้อน และใช้งานได้ยากหากผู้ใช้งานขาดความเข้าใจในระบบ SIEM หรือแนวทางการโจมตีระบบ เพื่อคุ้มค่า และต้องใช้ความเข้าใจกับความต้องการ และวัตถุประสงค์ขององค์กร จากภาพประกอบที่ 2.22 คือความสามารถหลักของ SIEM



ภาพประกอบที่ 2.22 แสดง การทำงานของ SEIMและความสามารถที่โดดเด่น

ที่มา : Cyfence.com, 2022

2.6.2 ความสามารถของระบบ Security Information & Event Management (SIEM)

1. การจัดเก็บข้อมูล Log SIEM

มีความสามารถในการจัดเก็บรวบรวมข้อมูลต่าง ๆ ที่ใช้ในการตรวจสอบความมั่นคงปลอดภัย โดยสามารถเก็บรวบรวมข้อมูลได้จากหลากหลายแหล่งที่มา ไม่ว่าจะเป็น Firewalls, Server, EDR, XDR หรือแหล่งข้อมูลความมั่นคงปลอดภัยอื่น ๆ ไปจนถึง Device หรือ Computer ที่มีการใช้งานในองค์กร (Cyfence.com, 2022)

2. การวิเคราะห์ตรวจสอบภัยคุกคาม (Threat Hunting and Detection)

นอกจากการเก็บรวบรวมข้อมูล SIEM ยังสามารถวิเคราะห์ หรือตรวจสอบช่องโหว่ของระบบต่าง ๆ ที่มีความซับซ้อนได้ ระบบอัตโนมัติสามารถเชื่อมโยงพฤติกรรม การกระทำ หรือกิจกรรมต่าง ๆ ที่เป็นความเสี่ยงให้เกิดภัยคุกคามทางไซเบอร์ได้ SIEM เป็นหัวใจในการทำ threat hunting (การไล่ล่าภัยคุกคาม) โดยการ Integrate SIEM เข้าสู่ศูนย์กลางการทำงานของ Threat Investigation Tools (เครื่องมือตรวจสอบภัยคุกคาม) ช่วยให้สามารถตรวจเจอภัยคุกคามที่อาจเกิดจะเกิดขึ้นได้ (Cyfence.com, 2022)

3. ติดตามภัยคุกคามได้แบบ Realtime

ระบบ SIEM ยังสามารถช่วยประหยัดเวลาในการค้นหาและระบุตำแหน่งของจุดอ่อนภายในระบบ ทำให้รู้ช่องโหว่ที่ต้องแก้ไขได้อย่างรวดเร็ว จากการวิเคราะห์ และแจ้งเตือนให้แก่ทีม CSOC เพื่อให้สามารถตรวจสอบกิจกรรม หรือระบบที่เกิดขึ้นได้อย่างทันทั่วทั้ง (Cyfence.com, 2022)

4. การจัดหมวดหมู่ Event ของภัยคุกคาม

SIEM สามารถจัดหมวดหมู่ของภัยคุกคาม ไม่ว่าจะเป็นภัยในอีเมลระบบคลาวด์ แอปพลิเคชัน แหล่งข้อมูลภายนอก พร้อมกับระบุตำแหน่งจุดเสี่ยงที่ต้องแก้ไขได้ (Cyfence.com, 2022)

5. ลดเวลา Response Time

การใช้ Enhance Situational Awareness ระบบของ SIEM สามารถใช้ประโยชน์จาก Threat Intelligence ทั่วโลก เพื่อสามารถค้นพบเหตุการณ์การสื่อสารที่น่าสงสัย หรือ Malicious IP ที่เป็นอันตราย พร้อมทั้งยังสามารถระบุตำแหน่งที่อาจถูกโจมตีได้ ลดเวลา Response Time สามารถจัดการภัยคุกคามที่ผลกระทบต่อระบบของเราอย่างรวดเร็วเช่นกัน

6. การทำงานร่วมกับระบบด้านความมั่นคงปลอดภัยอื่น ๆ

การทำงานร่วมกับระบบด้านความมั่นคงปลอดภัยอื่น ๆ เช่น SOAR EDR และ XDR เป็นต้น ทำให้การตรวจสอบเหตุการณ์ ช่องโหว่ ความเสี่ยง และค้นหาภัยคุกคาม มีประสิทธิภาพมากยิ่งขึ้น รวมไปถึงอาจใช้ระยะเวลาสั้นลงอีกด้วย

7. การแสดงผลข้อมูล Dashboard

การสามารถแสดงผลเป็น Dashboard ที่ง่ายสำหรับทีม CSOC หรือ Admin ในการเรียกดูข้อมูล Log, Alerts, ลำดับของเหตุการณ์ รวมไปถึงสามารถตรวจสอบในเชิงลึกได้ง่ายยิ่งขึ้น (Cyfence.com, 2022)



ภาพประกอบที่ 2.23 แสดง กระบวนการทำงานของ SIEM มีอะไรบ้าง
ที่มา : Cyfence.com, 2022

2.6.2 กระบวนการทำงานของ Security Information & Event Management (SIEM) ดังภาพประกอบที่ 2.23 ตามรายละเอียดดังนี้

1. การรวบรวมข้อมูล (Data Collection)

การรวบรวมข้อมูลจากแหล่งข้อมูลความมั่นคงปลอดภัยในระบบเครือข่ายทั้งหมด เช่น ข้อมูล Log ระบบปฏิบัติการ ซอฟต์แวร์ป้องกันไวรัส ระบบป้องกันการบุกรุก Server และ Firewall เพื่อทำการบันทึกข้อมูลเก็บไว้ก่อนนำไปวิเคราะห์หาจุดอ่อน ช่วยเหลือลดเวลาดำเนินงาน (Cyfence.com, 2022)

2. ข้อกำหนด (Policies)

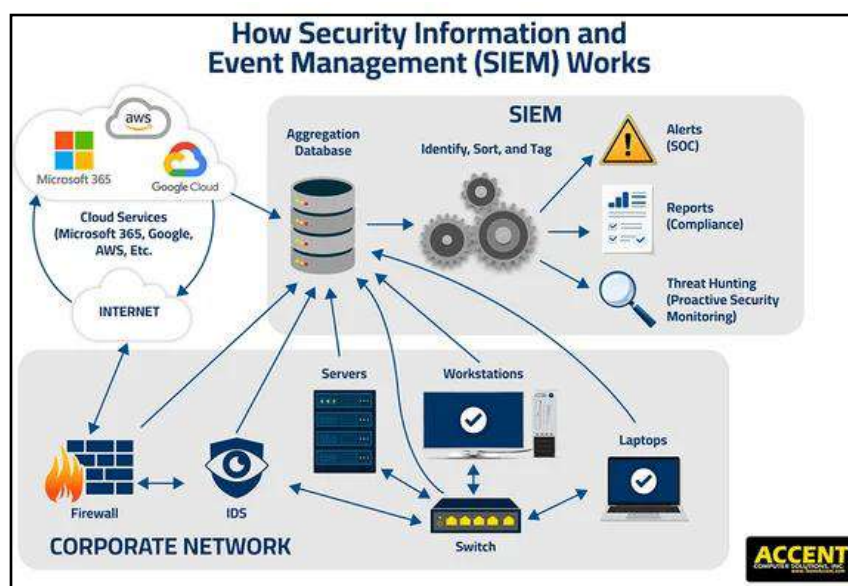
เป็นสิ่งที่ถูกสร้างโดย SIEM administrator เพื่อกำหนดพฤติกรรมของ Enterprise system (ระบบศูนย์กลางของทั้งองค์กร) ภายใต้สถานการณ์ปกติ และระหว่างเหตุการณ์ด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้น SIEMs มีความสามารถสร้าง default rules การแจ้งเตือน รีพอร์ต และแดชบอร์ดที่ปรับแต่งให้สอดคล้องกับความจำเป็นด้านความมั่นคงปลอดภัยที่เราต้องการเฉพาะ (Cyfence.com, 2022)

3. การจัดการความสัมพันธ์ (Data consolidation and correlation)

ระบบ SIEM จะจัดเรียงแปลงข้อมูล วิเคราะห์ และหาความสัมพันธ์ของ Log ต่าง ๆ ที่ทำการเก็บมา แล้วจัดประเภทข้อมูลและข้อกำหนด เพื่อให้ได้ตำแหน่งของจุดเสี่ยงที่อาจถูกภัยคุกคามทางไซเบอร์โจมตีได้ (Cyfence.com, 2022)

4. การแจ้งเตือน (Alerts & Notifications)

เมื่อมี Event หรือการกำหนดค่าของ Event Trigger กับ SIEM Rule ระบบจะแจ้งเตือนเจ้าหน้าที่ด้าน Security ซึ่งเป็นไปตามกระบวนการทำงาน ตามภาพประกอบที่ 2.24



ภาพประกอบที่ 2.24 แสดง How Security Information and Event Management (SIEM) Works

ที่มา : vc3.com, 2022

2.6.3 บทสรุปของ Security Information & Event Management (SIEM)

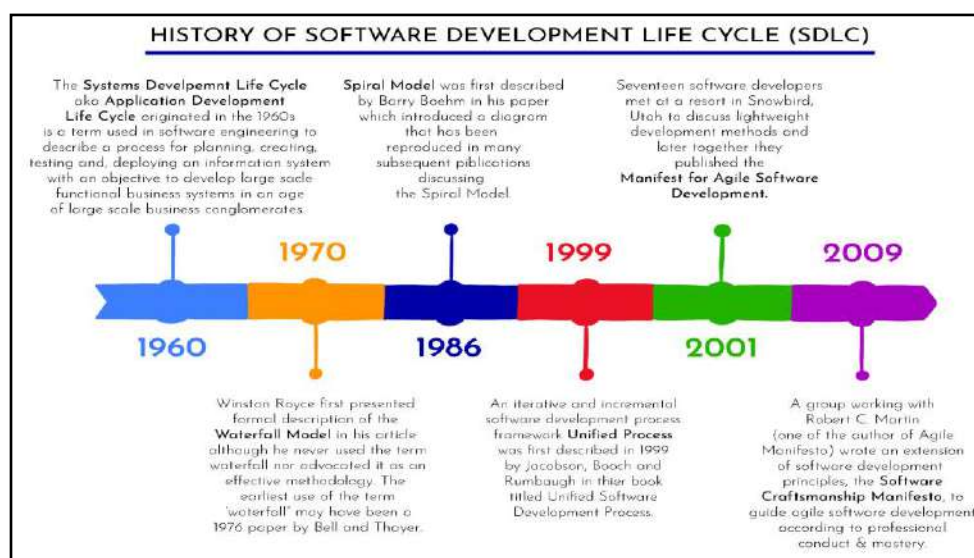
ระบบที่รวบรวมข้อมูลที่เกี่ยวข้องกับความมั่นคงปลอดภัยในลักษณะรวมศูนย์เพื่อตรวจจับภัยคุกคามหรือเหตุการณ์ให้ความสามารถในการวิเคราะห์ความมั่นคงปลอดภัยแบบเรียลไทม์หรือเหตุการณ์ที่ผ่านไปแล้วโดยการเชื่อมโยงเหตุการณ์บันทึกจำนวนหลายรายการ อีกทั้งยังมีฟังก์ชันต่างๆ เพื่อใช้ในการตรวจสอบความผิดปกติ เช่น การเพิ่มประสิทธิภาพด้วยข้อมูลบริบทที่เป็นปกติจากแหล่งข้อมูลที่แตกต่างกัน การรายงาน การแจ้งเตือน และความสามารถในการตอบสนองต่อเหตุการณ์

อย่างอัตโนมัติ เช่น การแจ้งเตือนหรือป้องกันการโจมตี ซึ่งช่วยให้สามารถแลกเปลี่ยนข้อมูลภัยคุกคามกับแพลตฟอร์มต่างๆ เพื่อแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์

SIEM ใช้เก็บข้อมูลแบบกระจายเพื่อนำข้อมูลออกมาอย่างมีประสิทธิภาพสำหรับการแยกข้อมูลเหตุการณ์ และประมวลผลข้อมูลล่วงหน้าสำหรับการตรวจจับเหตุการณ์ที่น่าสงสัยจากนั้นข้อมูลเหตุการณ์ที่ประมวลผลข้อมูลที่ถูกส่งออกมาจากอุปกรณ์เพื่อจัดเก็บ และการวิเคราะห์เพิ่มเติมครอบคลุมเพื่อระบุพื้นที่ที่มีความเสี่ยงสูง

2.7 หลักการวงจรการพัฒนาระบบ (System Development Life Cycle: SDLC)

กระบวนการพัฒนาระบบที่เป็นมาตรฐานที่ยอมรับในปัจจุบัน นั้นคือ วงจรการพัฒนาซอฟต์แวร์ หรือ Software Development Lifecycle (SDLC) คือกระบวนการที่คุ้มค่า และประหยัดเวลาในการออกแบบและสร้างซอฟต์แวร์ที่มีคุณภาพสูงสำหรับทีมนักพัฒนา โดยเป้าหมายที่สำคัญของกระบวนการ SDLC มีรูปแบบต่างๆ รวมถึง Waterfall, Spiral V-Model, Iterative และ Rapid Application Model วัตถุประสงค์หลักของ SDLC คือการลดโอกาสที่จะเกิดข้อผิดพลาดและปรับปรุงคุณภาพของผลิตภัณฑ์ซอฟต์แวร์ขึ้น จาก Timeline ดังภาพประกอบที่ 2.25

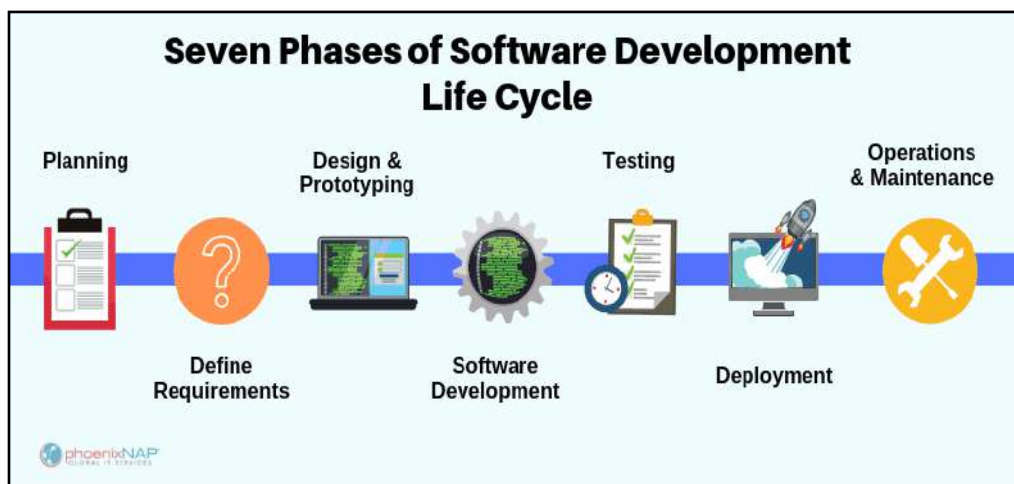


ภาพประกอบที่ 2.25 แสดง History Software Development Life Cycle

ที่มา : logic-fruit.com, 2023

2.7.1 ประวัติของ (System Development Life Cycle: SDLC)

ผู้วิจัยได้ทำการสืบค้น จากแหล่งอ้างอิงเว็บไซต์ www.logic-fruit.com เขียน โดย (Niranjana R, 2023) ได้กล่าวไว้ว่าในปี 1960 ขั้นตอนการพัฒนา ซึ่งเป็นที่รู้จักกันครั้งแรกในชื่อ “วงจรการพัฒนาระบบ” ตามที่ (Geoffrey Elliott, 2004) เขียนไว้ในหนังสือเรื่อง Global Business Information Technology โดยบริษัทขนาดใหญ่ได้สร้างแนวคิดนี้ขึ้นมา เพื่อช่วยในการจัดการระบบธุรกิจที่มีความซับซ้อนซึ่งต้องใช้การประมวลผล และการวิเคราะห์ข้อมูลเป็นจำนวนมาก วลีนี้ มีคำจำกัดความโดยสมบูรณ์ในปี 1971 โดยถูกนำไปใช้ครั้งแรกในทศวรรษ 1960 เมื่อคอมพิวเตอร์เมนเฟรมใช้พื้นที่ขนาดใหญ่ และมีความจำเป็นในการอธิบายขั้นตอนกระบวนการ รวมถึงเครื่องมือที่ใช้ในการสร้างระบบที่มีความซับซ้อน เพื่อตอบสนองความต้องการที่ซับซ้อนเช่นกัน ซึ่งความเปลี่ยนแปลงอยู่ตลอดเวลาของธุรกิจและผู้ใช้งาน สำหรับการพัฒนาระบบเทคโนโลยี ตามแนวทางดังภาพประกอบที่ 2.26



ภาพประกอบที่ 2.26 แสดง Seven Phases of Software Development Life Cycle

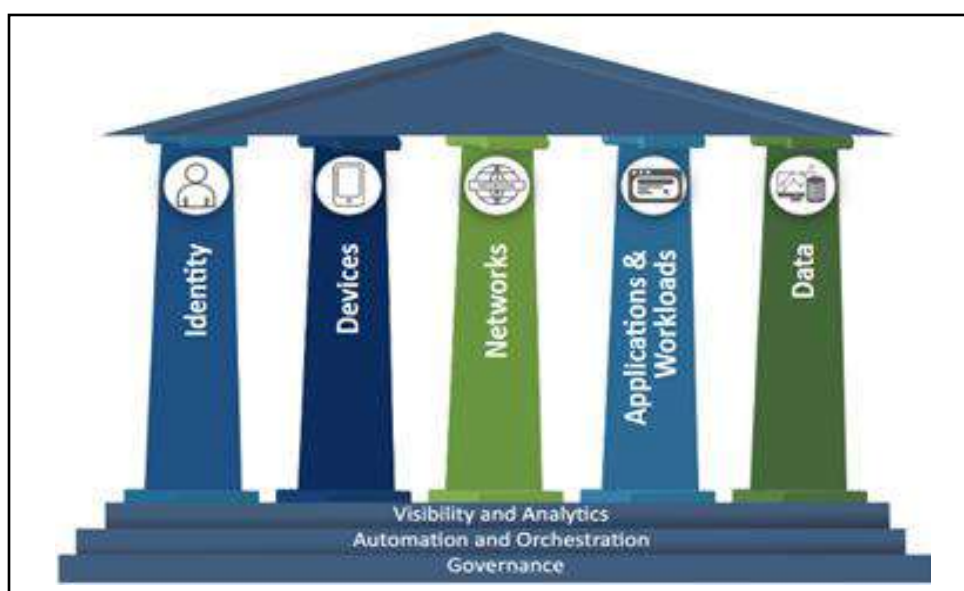
ที่มา : Devsquad.com, 2020

2.8 หลักการเกี่ยวกับ Zero Trust Architecture

ปัจจุบันของเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยข้อมูลที่มีแนวคิดความมั่นคงปลอดภัยแบบ Zero-Trust Model เป็นแนวทางที่เน้นความรอบคอบและควบคุมทุกด้านของการเข้าถึงข้อมูล และระบบ โดยไม่มีการให้ความเชื่อตัวเองโดยปกติ ในแนวคิดนี้ คำสำคัญคือ “Never trust, Always verify”

การเข้าถึงที่มาจากทั้งผู้ใช้งาน อุปกรณ์ เครือข่าย แอปพลิเคชัน และข้อมูลจากเครือข่ายภายนอกหรือภายในองค์กร ต้องผ่านการตรวจสอบเสมอ และได้รับสิทธิ์เท่าที่จำเป็น (Least Privilege) เท่านั้น

การควบคุมความมั่นคงปลอดภัยไซเบอร์ตามแนวคิด Zero Trust Architecture จะมีการออกแบบเพื่อปกป้องข้อมูลและบริการเป็นหลักโดยการรับรองความถูกต้องของอุปกรณ์ และผู้ใช้งานอย่างต่อเนื่อง, โดยไม่ให้ความเชื่อตัวเองโดยปกติ การเข้ารหัสทุกอย่างให้เป็นการเข้าถึงขั้นต่ำเท่าที่จำเป็น และมีการจำกัดระยะเวลาในการเข้าถึง การแบ่งส่วนการใช้งานเพื่อจำกัดความเสียหายกรณีมีการละเมิดข้อมูล โดยเฉพาะอย่างยิ่งข้อมูลที่อาจกระทบต่อความมั่นคงปลอดภัยของข้อมูล และความเป็นส่วนตัวของข้อมูล Data Privacy และ Data Security ดังรายละเอียดภาพประกอบที่ 2.27



ภาพประกอบที่ 2.27 แสดง Zero Trust Maturity Model Pillars

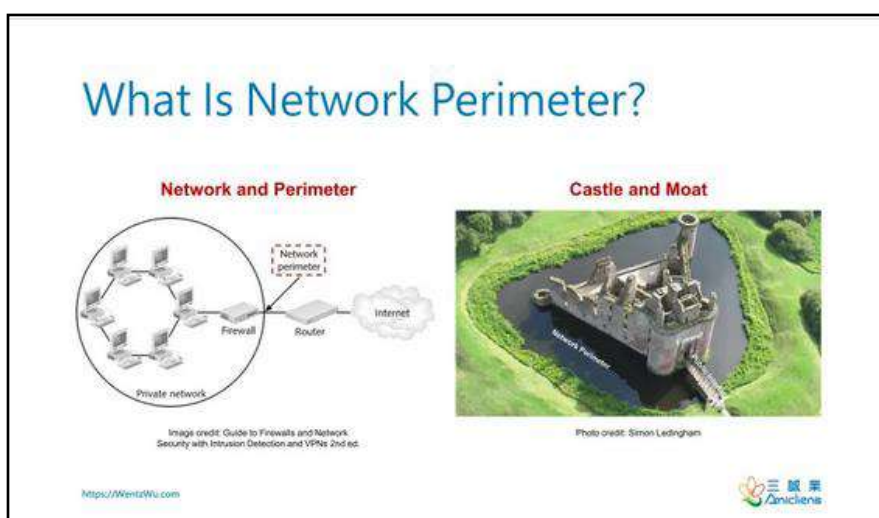
ที่มา : Cybersecurity and Infrastructure Security Agency, 2023

2.8.1 หลักการตามแนวคิด Zero Trust Architecture (ก.ล.ด., 2566) ตามภาพประกอบที่ 2.27 มีรายละเอียดดังนี้

1. แหล่งข้อมูลต่าง ๆ ถือเป็นสินทรัพย์สารสนเทศสำคัญขององค์กรที่ต้องได้รับการปกป้อง
2. ระบบเครือข่ายที่เชื่อมต่อจากทุกแห่งต้องมีความมั่นคงปลอดภัยเสมอ

3. ไม่ใช่การอนุญาตเพียงครั้งเดียวแล้วใช้ได้ทั้งหมด แต่ต้องได้รับอนุญาตให้เข้าใช้งานระบบงานข้อมูล หรือทรัพยากรใหม่ทุกครั้ง
4. กำหนดให้เข้าถึงการเข้าใช้ระบบงาน และข้อมูลสำคัญในลักษณะการยืนยันตัวตนแบบ Dynamic
5. หมั่นตรวจสอบการเข้าถึงการเข้าใช้ระบบงาน และข้อมูลสำคัญเป็นไปตามสิทธิ์
6. ปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยให้เป็นปัจจุบันอยู่เสมอ

ในปี 2010 John Kindervag จาก Forrester Research, Inc. เป็นผู้ริเริ่มแนวคิด Zero-Trust โดยนำมาประยุกต์ใช้ในการทำงานขององค์กร (linkedin.com , 2021) แนวคิดการจัดเก็บข้อมูลบนอินเทอร์เน็ตขององค์กรต้องมีการยืนยันตัวตนก่อนเข้าถึงข้อมูล โดยใช้คำว่า “Zero-Trust” เพื่อพิจารณา Network Topology เพื่อการพิสูจน์ตัวตนของผู้ใช้งานและอุปกรณ์ในเครือข่าย แนวคิด Zero-Trust นี้หากแบ่งเป็น 3 กลุ่มหลัก คือ ผู้ใช้งาน อุปกรณ์ และระบบซึ่งเป้าหมายคือเพิ่มความแข็งแกร่งให้กับระบบเครือข่ายและให้สิทธิ์การเข้าถึงข้อมูลขององค์กรได้อย่างสมบูรณ์ ตัวอย่างการประยุกต์ใช้หลักการนี้ได้แก่การใช้งานรีโมทเข้ามาจากระยะไกล และควบคุมการเข้าถึงเครือข่ายเพื่อควบคุมการเข้าถึงเครือข่ายอย่างเข้มงวดดังรายละเอียดภาพประกอบที่ 2.28

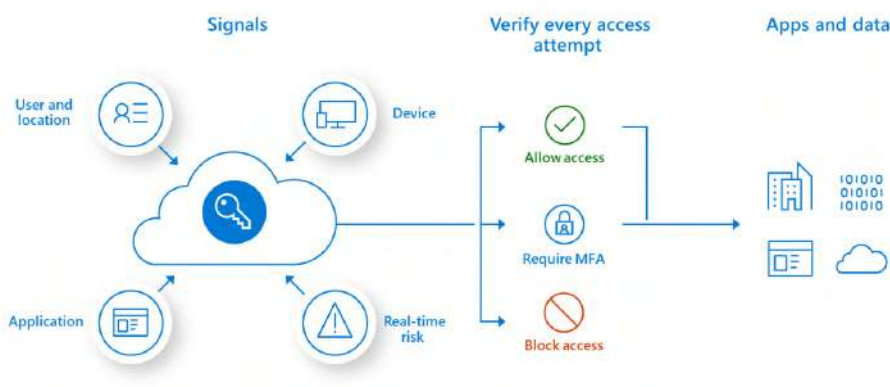


ภาพประกอบที่ 2.28 แสดง Network Castle and Moat Model

ที่มา : Wentzwu.com, 2021

จากภาพประกอบที่ 2.28 แสดงถึงการออกแบบเครือข่ายการป้องกันขององค์กรแบบเดิมและหลักการแบบเดิมได้ถูกกำหนดให้การเข้าถึงเพียงแค่ครั้งเดียวหลังจากนั้นการเข้าระบบทั้งหมดก็จะไม่ได้มีการตรวจสอบใด ๆ อีก ซึ่งส่งผลกระทบหากผู้ใช้งานขาดความเข้าใจเรื่องความมั่นคงปลอดภัยทางสารสนเทศ หรือความตระหนักในการป้องกัน อีกทั้งยังไม่ใส่ใจการทำงานที่ถูกต้องและเข้าใช้งานระบบที่ตัวเองไม่จำเป็น ก็ยิ่งเพิ่มความเสี่ยงต่อข้อมูล ซึ่งเป็นสิ่งสำคัญต่อองค์กร และเมื่อการตรวจสอบเพียงครั้งเดียว ยิ่งสะท้อนการป้องกันที่ไม่ปลอดภัยหาก มีการโจมตีเข้ามาในระบบขององค์กร ก็สามารถเข้าถึงทุกระบบในองค์กรได้อย่างอิสระ

การปรับใช้หลักการ Zero-Trust ยิ่งมีความสำคัญเนื่องจากการพัฒนาระบบไอทีที่ทันสมัยมีการเก็บข้อมูลในรูปแบบ Cloud หรือ SaaS การควบคุมการเข้าถึงข้อมูล และระบบจึงต้องปรับปรุงให้เข้ากับการเปลี่ยนแปลงในโครงสร้างของเครือข่ายไอทีในปัจจุบัน เพื่อให้รองรับการเก็บข้อมูลที่กระจายและรักษาความมั่นคงปลอดภัยของข้อมูล ตามภาพประกอบที่ 2.29



ภาพประกอบที่ 2.29 แสดง Network Zero Trust Model

ที่มา : Linkedin.com, 2023

จากแนวคิด ทำให้การเข้าถึงข้อมูลมีความเข้มงวด และตรวจสอบอยู่เสมอ เพื่อป้องกันให้ผู้ที่ไม่มีสิทธิ์หรือความเกี่ยวข้องกับระบบนั้นเข้าถึงข้อมูล และยังคงสภาพความมั่นคงปลอดภัยของข้อมูลให้เป็นไปตามสิทธิ์ที่ถูกต้องอยู่เสมอ จากแนวคิดของ (Ioan-Alexandru Dumitru, 2022) ได้กล่าวว่า ความมั่นคง

ปลอดภัยประเภท Zero Trust เป็นรูปแบบการรักษาความมั่นคงปลอดภัยด้านไอทีที่ต้องมีการยืนยันตัวตนอย่างเข้มงวดสำหรับทุกคนและอุปกรณ์ที่พยายามเข้าถึงทรัพยากรบนเครือข่าย เพราะการออกแบบที่ในรูปแบบปราสาท และคุณยายังคงมีจุดอ่อนเรื่องการป้องกันเพียงจุดเดียว ไม่ได้ไดนามิก ไปตามการใช้งานตามสิทธิ์การเข้าถึง และ ยังมีการกล่าวถึงในงานวิจัยของ (Mingyang Xu, Junli Guo, Haoyu Yuan และ Xinyue Yang, 2023) ว่า สถาปัตยกรรมความมั่นคงปลอดภัย Zero-trust สร้างรากฐานความไว้วางใจของการควบคุมการเข้าถึงขึ้นอยู่กับตรวจสอบสิทธิ์และการอนุญาตโดยการรับรองความถูกต้องของเทอร์มินัลอย่างต่อเนื่องในระหว่างกระบวนการตรวจสอบความถูกต้อง และยังสรุปว่า สถาปัตยกรรมความมั่นคงปลอดภัย Zero-Trust ชดเชยความเป็นจริงที่ว่าภัยคุกคามอาจอยู่ที่ใดก็ได้ และ ดังนั้นอินทราเน็ตขององค์กรของคุณไม่น่าจะปลอดภัยไปกว่าอินเทอร์เน็ต แม้จะมีชื่อ แต่ Zero Trust ก็มีความหมายว่าเกี่ยวกับความไว้วางใจมากกว่าแค่ความจริง

Zero Trust Architecture ให้สถาปัตยกรรมความมั่นคงปลอดภัยที่แข็งแกร่งขึ้นเพื่อป้องกันองค์กรและพร้อมการควบคุมการระบุตัวตน และการเข้าถึงปกป้องเพื่อธุรกิจจากภัยคุกคามทางไซเบอร์ทุกประเภท ไม่ว่าจะเป็นจากทั้งภายในและภายนอก ขององค์กร ถึงแม้การรักษาความมั่นคงปลอดภัยนี้จะมีความซับซ้อน และความยุ่งยากในการกำหนดให้ผู้ใช้งาน ก่อนเข้าทรัพยากร แต่การให้ความสำคัญในการตรวจสอบยังสร้างความน่าเชื่อถือหรือใช้ ระบบ Identity Credential และการจัดการการเข้าถึง และตรวจสอบแบบหลายเงื่อนไข เพื่อเป็นการควบคุมอีกชั้นหนึ่ง

Ms. Divya P. และ Sherin Sithara. A. (2022) ได้ความเห็นไว้ว่า Zero Trust เป็นโซลูชันที่ปลอดภัยที่กำลังได้รับความสนใจในด้านความมั่นคงปลอดภัยทางไซเบอร์โดยเฉพาะอย่างยิ่งเมื่อเผชิญกับการโจมตีทางไซเบอร์ที่เพิ่มขึ้นทั่วโลกมันให้สถาปัตยกรรมความมั่นคงปลอดภัยที่แข็งแกร่งขึ้นพร้อมตัวตนและการควบคุมการเข้าถึง ปกป้องธุรกิจจากภัยคุกคามทางไซเบอร์ทุกประเภทจากแหล่งทั้งภายใน และภายนอก ซึ่งเน้นการกำหนดสิทธิ์การตรวจสอบความมั่นคงปลอดภัยอย่างต่อเนื่อง และสม่ำเสมอ

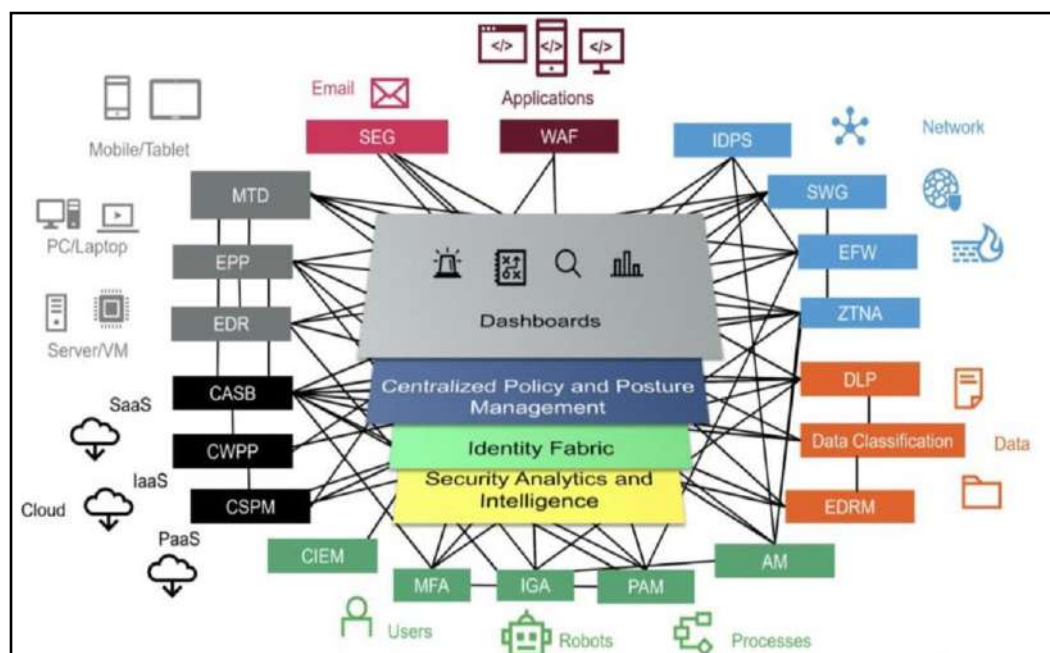
2.9 หลักการเกี่ยวกับ Cybersecurity Mesh Architecture

แนวคิดเกี่ยวกับ Cybersecurity Mesh Architecture เกิดจาก Gartner ในปี 2021 ได้ให้แนวคิดเกี่ยวกับเรื่องนี้ (Gartner.com, 2021) Cybersecurity Mesh Architecture หรือ CSMA เป็นหัวข้อการวิจัยที่เน้นการพัฒนาและการนวัตกรรมในด้านความมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กรสมัยใหม่ ระบบนี้

เป็นผลมาจากการรวมเครื่องมือรักษาความมั่นคงปลอดภัยแบบกระจายอย่างมีประสิทธิภาพ และมีการรวมกลยุทธ์ที่เชื่อมโยงระหว่างศูนย์ข้อมูล และส่วนควบคุมเพื่อเพิ่มประสิทธิภาพในการตรวจจับ และการตอบสนอง ระบบนี้ยังมียุทธศาสตร์ที่สอดคล้องกัน การจัดการที่ช่วยเพิ่มความสามารถในการควบคุม การเข้าถึงอย่างแม่นยำ และปรับเปลี่ยนได้ ทั้งหมดนี้มีผลทำให้องค์กรมีระบบความมั่นคงปลอดภัยที่ดีขึ้นในยุคสมัยที่ความสำคัญอย่างมากในองค์กร และภายนอกองค์กรเช่นกัน

2.9.1 Cybersecurity Mesh Architecture Concept

ซึ่งปัจจุบันมีการปรับตัวจากการทำงานในปัจจุบันที่ต้องการความรวดเร็ว และคล่องตัวมากขึ้น โดยโครงสร้างพื้นฐานการทำงาน Cybersecurity Mesh Architecture Concept แบ่งโครงสร้างออกเป็น 4 ส่วนดังภาพประกอบที่ 2.30 และอธิบายดังต่อไปนี้ (linkedin.com, 2023)



ภาพประกอบที่ 2.30 แสดง Cybersecurity Mesh Architecture Concept

ที่มา : Exclusive-networks.com, 2023

1. Security Analytics and Intelligence คือส่วนที่รวมกลุ่มโซลูชันที่ใช้เพื่อการรวบรวม วิเคราะห์ ข้อมูลภัยคุกคาม และการตอบสนองภัยอย่างเหมาะสมเพื่อรวบรวมเหตุการณ์ภัยคุกคามจากทาง Cyber เช่น SIEM หรือ SOAR จะให้การแจ้งเตือนภัยคุกคามได้แบบเรียลไทม์ เป็นต้น

2. Distributed Identity Fabric คือส่วนที่รวบรวมโซลูชันสำหรับการทำ Privilege Access Management เป็นศูนย์กลางในการทำงานนโยบาย Zero Trust เพื่อทำให้ความปละความมั่นคงปลอดภัย ในการยืนยันตัวตนขององค์กรมีศักยภาพในการดูแลอย่างทั่วถึงทุกช่องทาง ซึ่งรวมถึงการจัดการการให้ สิทธิผู้ใช้ การเข้าถึงแบบปรับเปลี่ยนได้ การพิสูจน์ตัวตน และระบบกระจายอำนาจ

3. Consolidated Policy and Posture Management การบริหารจัดการและการบังคับใช้นโยบาย ความมั่นคงปลอดภัยทางไซเบอร์ในสภาพแวดล้อมที่แตกต่างกัน เพื่อให้มั่นใจถึงนโยบายความมั่นคง ปลอดภัยที่สอดคล้องกัน เพื่อใช้ในการวางกฎ และนโยบายต่างๆ รวมถึงมอบสิทธิการเข้าถึงการ ปรับแต่งให้แก่บุคคลที่เกี่ยวข้องดูแลอย่างเหมาะสม และเป็นมาตรฐานในระบบรักษาความมั่นคง ปลอดภัย

4. Consolidated Dashboards โครงสร้างเดิมแบบ Silo ที่แต่ละโซลูชันแยกกันทำงานนั้น ทำให้มี Dashboard เป็นจำนวนมาก ส่งผลให้เกิดความซับซ้อนในการวิเคราะห์ และตอบสนองภัยคุกคาม ดังนั้น CSMA จึงเสนอให้ทำการ Integrate Dashboard ให้สามารถสื่อสารกันได้ในแพลตฟอร์มที่เป็นศูนย์กลาง เพื่อให้ทีม SOC ได้ทำงานอย่างมีประสิทธิภาพเพื่อดูและจัดการมาตรการรักษาความมั่นคงปลอดภัย ทั้งหมดขององค์กร

2.9.2 การใช้ปรับใช้ Cybersecurity Mesh Architecture ภายในองค์กร

1. องค์กรควรทำการวิเคราะห์ และเข้าใจองค์ประกอบของระบบ และความต้องการของความ มั่นคงปลอดภัยทางไซเบอร์ขององค์กร นี้ช่วยให้องค์กรสามารถกำหนดเป้าหมาย และกำหนดวิธีการใช้ งานอย่างถูกต้องการสร้างกรอบการทำงานแบบรวมที่โซลูชันด้านความมั่นคงปลอดภัยสามารถทำงาน ร่วมกันเพื่อให้เกิดการทำงานรวมกันได้

2. การเลือกโซลูชันความมั่นคงปลอดภัยที่มีกรอบนโยบายที่กำหนดเพื่อให้แน่ใจว่าเข้ากันได้กับ กรอบงานโดยรวมมากกว่าอุปกรณ์ต่างๆ และสอดคล้องเป็นไปตามนโยบายต่างๆ

3. การปรับใช้การเข้าถึงเครือข่ายแบบ Zero Trust ที่รวมเข้ากับเครื่องมือการจัดการเข้าถึงเครือข่าย และระบบการทำงานต่างๆ ผ่านรีโมทระยะไกลหรือ VPN แบบดั้งเดิมเพื่อความน่าเชื่อถือ และความมั่นคงปลอดภัยของระบบสารสนเทศมากยิ่งขึ้น

4. กระบวนการและขั้นตอนการตรวจสอบที่เหมาะสมซึ่งเป็นไปตามกรอบ Zero Trust เพื่อให้เฉพาะผู้ใช้งานนั้นซึ่งได้รับอนุญาตตามความเหมาะสมที่สามารถเข้าถึงระบบขององค์กรได้อย่างถูกต้อง และปลอดภัย

2.9.3 ประโยชน์ด้านเชิงกลยุทธ์ของ Cybersecurity Mesh Architecture (Stefanini.com, 2021)

1. Cybersecurity mesh จะรองรับระบบ Identity and Access Management (IAM) มากกว่า 50% ในปัจจุบัน โดยที่ส่วนใหญ่ของสินทรัพย์ด้านดิจิทัล และอุปกรณ์ที่อยู่ภายนอกขององค์กร ทำให้การรักษาความมั่นคงปลอดภัยทางสารสนเทศที่มีความซับซ้อน เมื่อปรับใช้ Identity and Access Management ด้วย Cybersecurity Mesh โดยองค์กรจะได้รับแนวทางที่บูรณาการ และมีความยืดหยุ่นที่น่าเชื่อถือได้มากขึ้น ในการควบคุมการเข้าถึงสินทรัพย์ดิจิทัล มากกว่าการควบคุมรักษาความมั่นคงปลอดภัยแบบเดิมๆ ที่ใช้กันอยู่ทั่วไปในปัจจุบัน

2. การบริการ Identity and Access Management จะส่งผลให้ผู้ให้บริการรักษาความมั่นคงปลอดภัยที่มีการจัดการ Managed Security Service Providers (MSSP) มีจำนวนเพิ่มขึ้น ซึ่งสามารถจัดหาทรัพยากรที่มีคุณภาพ และทักษะที่จำเป็นต่อองค์กรเพื่อวางแผนพัฒนา และนำไปปรับใช้ Identity and Access Management ที่ครอบคลุมมากขึ้น ซึ่งทาง Gartner ได้มีการคาดการณ์ว่าภายในปี 2566 จำนวน 40% ของจำนวนรวมแอปพลิเคชัน Identity and Access Management จะถูกใช้ขับเคลื่อนโดย MSSP เป็นหลัก

3. เครื่องมือพิสูจน์ตัวตนจะถูกเพิ่มเข้าไปในวงจรการระบุตัวตนของผู้ใช้งานระบบต่างๆ ซึ่งขั้นตอนการลงทะเบียน และการกู้คืนข้อมูลที่มีประสิทธิภาพมากขึ้นและมีความจำเป็นเร่งด่วน เนื่องจากการรีโมทระยะไกลที่เพิ่มขึ้นอย่างมากอย่างต่อเนื่องจากการใช้งาน WFH ในปัจจุบัน ซึ่งทำให้ยากต่อการแยกความแตกต่างระหว่างผู้โจมตีและผู้ใช้ที่ถูกต้อง ซึ่งทาง Gartner ระบุว่าภายในปี 2567 จำนวน 30% ขององค์กรขนาดใหญ่ จะใช้เครื่องมือพิสูจน์ตัวตนใหม่ๆ เพื่อแก้ไขจุดอ่อนในกระบวนการระบุตัวตนของพนักงาน ที่ใช้ระบบระยะไกลมากขึ้น

4. มาตรฐานการระบุตัวตนแบบกระจายอำนาจเกิดขึ้น และรวมศูนย์สำหรับการจัดการข้อมูลประจำตัวทำให้การให้ความเป็นส่วนตัวมากขึ้น อีกทั้งการรับรอง ทำให้การแบ่งตัวนั้นทำได้ยากยิ่งขึ้น ด้วยวิธีการกระจายอำนาจที่ได้รับการสนับสนุนจากโมเดลนี้ ทำให้ Blockchain Technology จะเป็นส่วนการประกันความเป็นส่วนตัว และช่วยให้สามารถตรวจสอบคำขอข้อมูลได้ถูกต้อง

2.9.4 สรุปการเกี่ยวกับ Cybersecurity Mesh Architecture

Cybersecurity Mesh Architecture เป็นกลยุทธ์การป้องกันทางไซเบอร์แบบกระจายตัวที่ปกป้องเครือข่ายองค์กรโดยการสร้างขอบเขตที่อยู่รอบ ๆ ในแต่ละอุปกรณ์ได้ตามคุณสมบัติ Flexibility, Agile และ Scalable แทนที่จะสร้างการรักษาความมั่นคงปลอดภัยในขอบเขตเดียวแบบเดิม และเป็นการป้องกันเดียวที่ใช้ร่วมกันทั้งหมด สำหรับทั้งเครือข่าย ซึ่งหาก Cyber Security Mesh Architecture (CSMA) มี 4 เลเยอร์ในการกำหนดค่าตามที่กล่าวมาข้างต้น และจัดการบริการรักษาความมั่นคงปลอดภัยที่แตกต่างกัน อีกทั้งการวิเคราะห์ข้อมูลความมั่นคงปลอดภัย โครงสร้างข้อมูลประจำตัวแบบกระจาย การจัดการทางนโยบายแบบรวมศูนย์ และแดชบอร์ดแบบรวมศูนย์ Cyber Security Mesh Architecture เป็นสถาปัตยกรรมมีความท้าทาย และมุ่งสู่การปรับตัวต่อการเปลี่ยนแปลงทางไซเบอร์อย่างมีประสิทธิภาพโดยมีความพร้อมต่อการรองรับภัยคุกคามทางไซเบอร์ในยุคสมัยใหม่ ที่ความมั่นคงปลอดภัยทางไซเบอร์มีความสำคัญเป็นอย่างมากสำหรับภายใน และภายนอกองค์กร เช่นกัน

2.10 งานวิจัยที่เกี่ยวข้อง

2.10.1 งานวิจัยภายในประเทศ

นิลमित นิลาศ (2560) งานวิจัยกล่าวว่า Mirai Botnet ก่อให้เกิดผลกระทบอย่างมีนัยสำคัญต่อระบบอินเทอร์เน็ตส่งผลให้ลูกค้าของ Deutsche Telekom มากกว่า 90,000 รายไม่สามารถเข้าถึงอินเทอร์เน็ตได้ โดยปริมาณการส่งข้อมูล (Bandwidth) โดยรวมสูงถึง 1 TB ต่อวินาทีในระหว่างการโจมตี DDoS กำหนดเป้าหมายอุปกรณ์ IoT เช่นกล้องไอพีที่ใช้ซีพียู (CPU) เป็นแบบ ARM, ARM7, Motorola 6800, SPC, PowerPC, X86 และ SuperH (SH4) โดยซอร์สโค้ดของ Mirai จะประกอบด้วย 16 ไฟล์ที่มีฟังก์ชัน 138 รายการ รวมถึงบัญชีผู้ใช้และรหัสผ่าน 62 ชุด Mirai Botnet ใช้เทคนิคฟLOODING (Flooding) มากกว่า 9 วิธี สำหรับการโจมตีพอร์ต โดยเฉพาะเป้าหมายพอร์ต 22, 23 และ 80 เพื่อเป็นการ

ป้องกันการโจมตี จึงแนะนำให้ปิดใช้งานพอร์ต 22, 23 และ 80 บนอุปกรณ์กล้องไอพีหรือใช้เทคนิคการ
ใช้งานที่เหมาะสม

ธริช พงษ์รชนี (2562) กล่าวถึงการพัฒนาระบบ Mini SOC (Security Operations Center) สำหรับ Web server โดยมุ่งเน้นไปที่การตรวจจับและป้องกันภัยคุกคามระบบใช้เทคโนโลยี SIEM (Security Information and Event Management) เพื่อตรวจสอบ และวิเคราะห์กิจกรรมบน Web server ระบบ Mini SOC มีจุดมุ่งหมายเพื่อเพิ่มความมั่นคงปลอดภัยโดยการระบุ และตอบสนองต่อภัยคุกคามที่อาจเกิดขึ้นได้แบบเรียลไทม์ความสำคัญของการวิเคราะห์สาเหตุรากในการระบุสาเหตุพื้นฐานของเหตุการณ์ด้านความมั่นคงปลอดภัยความสามารถในการตรวจสอบ และวิเคราะห์แบบเรียลไทม์เพื่อตรวจจับ และลดความเสี่ยงด้านความมั่นคงปลอดภัย

ณิชาธิ์ ลิมปนเทวินทร์ และพัชนี เสงี่ยมรักษา (2562) ศึกษาวิจัยระบุว่าผู้ตอบแบบสอบถามส่วนใหญ่ในการศึกษาเป็นผู้หญิงอายุระหว่าง 20-25 ปีและแสดงพฤติกรรมเช่นชอบโพสต์ตรวจสอบ และแบ่งปันข้อมูลส่วนบุคคลบนโซเชียลมีเดียพบว่าผู้เข้าร่วม Generation Y ใช้โซเชียลมีเดียเป็นหลักหลังทำงานจนถึงเวลากลางคืน ระหว่าง 19:00-23:59 น. การศึกษาระบุว่ามีเพียงสองปัจจัยคือพฤติกรรมโซเชียลมีเดีย และการรู้สึสามารถใช้ในการทำนายปัจจัยความมั่นคงปลอดภัยของความมั่นคงปลอดภัยทางไซเบอร์

ฐกฤต แก้วทับทิม (2564) ได้ศึกษาวิจัยเรื่อง การสังเกตการณ์การเพิ่มขึ้นของอาชญากรรมไซเบอร์ในระหว่างวิกฤต COVID-19 ที่เกี่ยวข้องกับการเพิ่มการใช้งานอินเทอร์เน็ต และข้อจำกัดที่เกิดจากการระบาด COVID-19 เป็นที่สำคัญ โดยการรวบรวมเรื่องราวข้อมูลทางอาชญากรรมไซเบอร์ในยุคปัจจุบัน และเกิดความเชื่อมโยงระหว่างการทำอาชญากรรมทางไซเบอร์ที่ร่วมมือกันเพื่อผลประโยชน์ร่วมกัน จากสถานะการณ์การระบาดโรค COVID-19 รวมถึงภาวะการปฏิเสธทางอินเทอร์เน็ต การระบาดไวรัสซัสแมร์ การโกงการซื้อขายผ่านระบบออนไลน์ และการละเมิดสิทธิมนุษยชน ซึ่งเป็นสิ่งที่ต้องตระหนักให้มีความสนใจ และเข้าใจเปรียบเทียบและวิเคราะห์ความสัมพันธ์ระหว่างพวกนี้ในระหว่างสถานการณ์เหล่านี้ ที่ส่งผลต่อความมั่นคงปลอดภัยของข้อมูล และระบบไซเบอร์อย่างรวดเร็ว และซับซ้อน

กฤษณะ นิยมณี และมณีนุช โชติรุ่งรัตน์ (2564) ได้ศึกษาวิธีป้องกันสินทรัพย์ไซเบอร์จากแรนซัมแวร์โดยทบทวนวรรณกรรมที่เกี่ยวข้อง และกรณีศึกษาจริงของการโจมตีทางไซเบอร์จากแก๊ง Maze

เผยให้เห็นว่าพวกเขาใช้เทคนิคที่คล้ายกันเช่น การรักษาฐาน และเข้าซ่อนตัวในเครือข่ายคอมพิวเตอร์ก่อนที่จะดำเนินการเข้ารหัสข้อมูล และหากระบบตรวจสอบการป้องกันที่มีประสิทธิภาพ ก็จะสามารถช่วยตรวจจับ และป้องกันภัยคุกคามทางไซเบอร์อันเป็นที่น่าสงสัยนี้ได้ บทความได้นำเสนอแนวทางสำหรับการป้องกันแรนซัมแวร์ Maze นี้ว่า การกำหนดค่าประเมินความมั่นคงปลอดภัยทางไซเบอร์ ระบบการป้องกันข้อมูล ที่มีความสามารถในการตรวจจับภัยคุกคาม ที่เข้ามาทางไซเบอร์ และการตอบสนองต่อภัยคุกคามที่เข้ามา รวมถึงการกู้คืนข้อมูลหลังจากการรับการคุกคาม

กรกัญญ์ญารัก บุญสุขเกิด (2564) ได้ศึกษาวิวัฒนาการของภัยคุกคามทางไซเบอร์และอาชญากรรมไซเบอร์ในประเทศไทย เน้นถึงความจำเป็นในการพัฒนาระบบกฎหมายเพื่อควบคุมอาชญากรรมทางคอมพิวเตอร์ เน้นถึงความสำคัญของการปรับปรุง และบังคับใช้พระราชบัญญัติความมั่นคงปลอดภัยทางไซเบอร์ปี 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล 2562 เพื่อปกป้องโครงสร้างพื้นฐานด้านข้อมูลที่สำคัญ และความเป็นส่วนตัวของบุคคลแม้จะมีการพัฒนากฎหมาย แต่ก็ยังมีช่องว่างในการจัดการกับอาชญากรรมคอมพิวเตอร์เนื่องจากวิวัฒนาการของเทคโนโลยีอย่างต่อเนื่องและชี้ให้เห็นว่าทักษะการดำเนินงานของพนักงานควรได้รับการปรับปรุง และนำไปใช้ในองค์กรทั้งภาครัฐ และเอกชนเพื่อป้องกันและจัดการกับภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ

เอกชัย พ่วงพรพิทักษ์ และคณะ (2565) งานวิจัยนี้ได้สรุปเกี่ยวกับพัฒนาแนวทางสำหรับการสอบสวนอาชญากรรมไซเบอร์ในบริบทการอิเล็กทรอนิกส์ และวิเคราะห์เทคนิคเทคโนโลยีสารสนเทศเพื่อสร้างต้นแบบที่ได้รับการปรับปรุงด้านความมั่นคงปลอดภัยได้แก่ แนวทางการสอบสวนอาชญากรรมที่มีประสิทธิภาพ การวิเคราะห์เทคนิคความมั่นคงปลอดภัยทางไซเบอร์เพื่อปรับปรุงการสอบสวนอาชญากรรม และการออกแบบและพัฒนาระบบต้นแบบระบบเพื่อเพิ่มความมั่นคงปลอดภัยของระบบธนาคารอิเล็กทรอนิกส์ ความซับซ้อนของกฎหมาย และการสอบสวนอาชญากรรม และความจำเป็นในการรวมความสามารถของผู้ตรวจสอบอาชญากรรม และช่างเทคนิคด้านความมั่นคงปลอดภัยด้านไอที บทความกล่าวถึงเทคนิค และเครื่องมือต่าง ๆ ที่ใช้ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เช่น SSL Strip, DROWN, POODLE, Homograph ฟิชชิง, Marlinpike, Dsniff, Bettercap, Ettercap, Wireshark, TCPDump, HProxy, https Lock, ISAN-HTTPS Enforcer, Click2Enforce และ HTTP Strict Transport Security (HSTS)

ธนพงศ์ ฉันทวิเชียร (2566) ได้การวิจัยวิเคราะห์ภัยคุกคามปัจจัยเสี่ยงและการปฏิบัติในปัจจุบันของการจัดการความเสี่ยงภัยคุกคามทางไซเบอร์ในหมู่หน่วยงานตุลาการภายใต้เขตอำนาจศาลของประธานศาลภาค 9 การศึกษาระบุปัจจัยเสี่ยงภัยคุกคามทางไซเบอร์ที่หน่วยงานเหล่านี้เผชิญรวมถึงซอฟต์แวร์โปรแกรมที่ดาวน์โหลดฟรี การเชื่อมต่ออินเทอร์เน็ตไร้สาย สภาพแวดล้อมที่เปิดเผย การโจมตีโดยไม่ได้ตั้งใจ และการโจมตีโดยเจตนา ความสำเร็จของการจัดการความเสี่ยงภัยคุกคามทางไซเบอร์ในกลุ่มหน่วยงานเหล่านี้ ได้แก่ การกำหนดระดับการเข้าถึงความถูกต้อง และความถูกต้องของข้อมูลและความพร้อมในการป้องกันภัยคุกคามทางไซเบอร์สำหรับทั้งซอฟต์แวร์และฮาร์ดแวร์ การศึกษายังระบุอุปสรรคที่ขัดขวางการจัดการความเสี่ยงภัยคุกคามทางไซเบอร์ เช่น งบประมาณที่ไม่เพียงพอสำหรับการจัดหาซอฟต์แวร์ และฮาร์ดแวร์ขาดความรู้ และทักษะในหมู่บุคลากร บุคลากรด้านไอทีหรือไซเบอร์ไม่เพียงพอ สถานที่ใกล้ชายฝั่ง และความซับซ้อนของระบบ มีการเสนอคำแนะนำสำหรับการจัดการความเสี่ยงภัยคุกคามทางไซเบอร์ที่ดีขึ้น รวมถึงการจัดสรรงบประมาณมากขึ้นสำหรับการประเมินความเสี่ยง และการประกันภัยการฝึกอบรมบุคลากรเพิ่มบุคลากรด้านไอทีหรือไซเบอร์การเปลี่ยนสถานที่และการลดความซับซ้อนของระบบ

2.10.2 งานวิจัยต่างประเทศ

Barbara Filkins (2019) บทความกล่าวถึง การประเมินผล โครงการ และการจัดซื้อจัดจ้างเป็นส่วนสำคัญสำหรับการใช้โซลูชัน SIEM แบบ (Next-Generation SIEM) โดยสาระสำคัญการลงทุนขององค์กรมิได้หยุดอยู่ที่การใช้งาน SIEM ที่ติดตั้งแล้วเท่านั้น แต่เพราะผู้โจมตีไม่เคยหยุดนิ่งพัฒนาวิธีการโจมตีที่มีความซับซ้อนมากขึ้น ดังนั้นจำเป็นต้องพัฒนาต่อไปให้ก้าวหน้า ผู้ที่ไม่หวังดีไปหนึ่งก้าว หรือกล่าวอีกนัยหนึ่ง คือต้องอยู่ด้านผู้นำการป้องกันต่อไปของการเปลี่ยนแปลง องค์กรจึงมีความจำเป็นต้องมีการปรับปรุงอย่างต่อเนื่อง ซึ่ง SIEM ยุคใหม่ช่วยให้สามารถวัดผล ที่ทราบถึงความพร้อมด้านความมั่นคงปลอดภัยขององค์กรและให้คำแนะนำเกี่ยวกับวิธีการปรับปรุงทั้งด้านบุคลากร กระบวนการ และเทคโนโลยี ซึ่งเป็นคุณสมบัติสำคัญของ SIEM แบบ (Next-Generation SIEM)

Sicone Zhang, Xiaoyao Xie และYang Xu (2020) ได้ศึกษาวิธีการใหม่ที่เรียกว่าวิธีการโจมตีแบบรุนแรงเพื่อประเมินความแข็งแกร่งของตัวจำแนกประเภทการเรียนรู้ของเครื่องในการรักษาความมั่นคงปลอดภัยทางไซเบอร์กับตัวอย่างที่ต่อสู้กัน สามารถใช้เพื่อประเมินความแข็งแกร่งของระบบการ

เรียนรู้ของเครื่องต่างๆในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงระบบตรวจจับการบุกรุกของโฮสต์ ระบบตรวจจับมัลแวร์ Android และระบบตรวจจับการบุกรุกเครือข่าย

Karel Hynek, Tomas Benes, Tomas Cejka และ Hana Kubatova (2020) เป็นการศึกษาวิจัยวิธีการใหม่ในการตรวจจับการโจมตีแบบ SSH Brute-force ที่เรียกว่า SSHCure ในเครือข่ายความเร็วสูง โดยใช้การเรียนรู้ของเครื่อง ซึ่งแบ่งออกเป็น 3 ขั้นตอน Scan, Brute-force และ Die-off สำหรับการประเมินโซลูชันโดยใช้ข้อมูล NetFlow เพื่อการตรวจจับที่มีความแม่นยำสูง และอัตรา (FP) ต่ำในการตรวจจับผู้โจมตี SSH Brute-force เพื่อหาแนวทางที่ดีขึ้นในการตรวจจับการโจมตี Brute-force ในระดับเครือข่าย เพื่อเพิ่มความแม่นยำในการรักษาความมั่นคงปลอดภัย

Scott Rose, Oliver Borchert, Stu Mitchell และ Sean Connelly (2020) มีความเห็นเกี่ยวกับ ZTA หรือ Zero Trust Architecture เป็นกระบวนการความมั่นคงปลอดภัยของเครือข่ายที่มุ่งเน้นไปที่ทรัพยากรแต่ละกลุ่ม แทนที่จะเป็นขอบเขตเครือข่ายที่กว้างไม่ให้ความไว้วางใจโดยนัยตามตำแหน่งทางกายภาพหรือเครือข่าย แต่ต้องมีการตรวจสอบสิทธิ์ก่อนที่จะให้การเข้าถึงทรัพยากรข้อมูล Zero Trust Architecture เป็นการตอบสนองต่อแนวโน้มเครือข่ายองค์กร เช่น ผู้ใช้ระยะไกลและการเข้าถึงบริการบนคลาวด์ที่ไม่ได้อยู่ภายในขอบเขตเครือข่ายขององค์กร โมเดลการปรับใช้ Zero Trust Architecture อาจรวมถึงโมเดลเกตเวย์เอนต์อุปกรณ์หรือแบบจำลองที่ส่วนประกอบเกตเวย์ ซึ่งอยู่ที่ขอบเขตของแหล่งทรัพยากรในแบบจำลองนี้ การรับส่งข้อมูลทั้งหมดจะถูกตรวจสอบ และลงชื่อเข้าใช้บนเครือข่าย แต่ปริมาณการใช้งานบางอย่างอาจวิเคราะห์เครือข่ายส่วนประกอบ Zero Trust Architecture สามารถดำเนินการภายในองค์กรหรือบริการบนคลาวด์ แนวทางที่ได้รับการปรับปรุงตามข้อมูลซึ่งมักใช้ในการปรับใช้กับ Zero Trust Architecture และกรณีการใช้งานที่ Zero Trust Architecture ก็สามารถทำให้สภาพแวดล้อมขององค์กรปลอดภัยยิ่งขึ้น เช่น รีโมตระยะไกล บริการคลาวด์ และบริการเครือข่ายสำหรับลูกค้า

Naeem Syed, Syed Shah, Arash Shaghaghi, Adnan Anwar, Zubair Baig และ Robin Doss (2021) ได้มีการสรุปทบทวนเอกสารมากกว่า 180 บทความที่มีความเกี่ยวข้องกับ Zero Trust โดยได้สรุปได้ว่า บทความนี้ให้การสำรวจที่ครอบคลุมเกี่ยวกับกระบวนการเชื่อมั่นความมั่นคงปลอดภัย Zero Trust (ZT) โดยกล่าวถึงหลักการพื้นฐาน ตัวเลือกที่เป็นไปได้สำหรับการตระหนักรู้ และเทคนิคที่ล้ำสมัยสำหรับการตรวจสอบความถูกต้องการควบคุมการเข้าถึงการเข้ารหัสการแบ่งส่วนขนาดเล็ก และ

ระบบอัตโนมัติด้านความมั่นคงปลอดภัย นอกจากนี้ยังเน้นถึงความท้าทายที่เกี่ยวข้องกับกลไกการรับรองความถูกต้อง รวมแผนการควบคุมการเข้าถึงทางเทคนิค ความน่าเชื่อถือและความเสี่ยง จากแนวทางการแบ่งกลุ่มและข้อกำหนดโดยซอฟต์แวร์ ซึ่งอาจส่งผลกระทบต่อการใช้งาน Zero Trust หลักการพื้นฐานของ Zero Trust Architecture จะเน้นประเด็นที่เกี่ยวข้องการตระหนักถึง Zero Trust Architecture โดกลุ่มเป้าหมายสำคัญสำหรับบทความนี้ คือการพัฒนาวิจัยด้านความมั่นคงปลอดภัยทางไซเบอร์และให้ข้อมูลพื้นฐานเกี่ยวกับ Zero Trust Architecture เพื่อนำเสนอแนวทางปฏิบัติที่ทันสมัย และช่วยระบุปัญหาในปัจจุบัน และนำเสนอทิศทางการวิจัยในอนาคตด้วยหลักการ Zero Trust Architecture

Jeonghoon Park, Jinsu Kim, B. B. Gupta และ Namje Park (2021) ได้วิจัยจำลองเพื่อตรวจสอบการโจมตี SSH แบบรุนแรงผ่านบันทึกเครือข่ายและควบคุมการเข้าถึงจากที่อยู่ไอพี ที่โจมตีมันแยก และแยกข้อมูลเฉพาะจากแพ็คเกจเรเตอร์ที่รวบรวมเพื่อตรวจสอบการโจมตีอินพุต SSH โดยไม่เลือกปฏิบัติแบบจำลองการเข้าถึงของผู้ใช้ในแต่ละแพ็คเกจด้วยน้ำหนัก และเพิ่มลงในบัญชีกำหนดตามค่าผลลัพธ์ที่คำนวณขั้นสุดท้ายนอกจากนี้ยังสามารถระบุไอพี ภายในของความพยายามโจมตี และป้องกันที่อยู่ IP ปลายทาง 29 อันแรกที่ยพยายามโจมตี

การวิจัยยืนยันว่าบันทึกจำนวนมากที่สร้างขึ้นในเรเตอร์เกิดจากการโจมตี SSH แบบ Brute-Force แบบจำลองการกำหนดไอพี ในรายการควบคุมโดยการแยกส่วน และตรวจสอบบันทึก ซึ่งสามารถป้องกันการโจมตีได้อย่างต่อเนื่องโดยการตรวจสอบการเข้าถึงของไอพี ภายในที่ผ่านเรเตอร์ไม่ได้ นอกจากนี้ยังสามารถป้องกันการเข้าถึงไอพีภายใน และโจมตีไอพี ของเว็บไซต์ โดยไม่ได้รับอนุญาตจากการสร้างรายการควบคุม ตามความเสี่ยงซึ่งจะป้องกันการไปยังระบบอื่น อย่างไรก็ตาม วิธีนี้ยังไม่มีความสามารถในการตอบสนองต่อการโจมตีแบบเรียลไทม์ และชี้ให้เห็นถึงความจำเป็นในการกำหนดบันทึกแบบเรียลไทม์โดยใช้การเรียนรู้ของเครื่องในอนาคต

Ms. Divya P และ Sherin Sithara. A (2022) มีความเห็นเกี่ยว Zero Trust โดยสรุปดังนี้ Zero Trust ให้สถาปัตยกรรมความมั่นคงปลอดภัยที่แข็งแกร่งโดยดำเนินการตรวจสอบอุปกรณ์ และผู้ใช้อย่างต่อเนื่องในแต่ละจุดเชื่อมต่อพร้อมกับการควบคุมตัวตน และการเข้าถึงสำหรับข้อมูลและกระทำธุรกรรมเน้นความจำเป็นในการตรวจสอบสิทธิ์อุปกรณ์ และผู้ใช้ทั้งหมดทั้งภายใน และภายนอกเพื่อป้องกันภัยคุกคามทางไซเบอร์ต่างๆ แนวคิดของ “Never Trust, Always Verify” ถูกเน้นว่าเป็นหลักการ

สำคัญของ Zero Trust โดยเน้นถึงความสำคัญของการตรวจสอบอย่างต่อเนื่องและการไม่มีโซน ข้อมูลประจำตัว หรืออุปกรณ์ที่เชื่อถือได้ Zero Trust ได้รับการยอมรับว่าเป็นโซลูชันที่มีแนวโน้มที่จะตอบสนองความต้องการด้านความมั่นคงปลอดภัยเครือข่ายที่พัฒนาขึ้น โดยนำเสนอการตรวจสอบสิทธิ์ การควบคุมการเข้าถึงและความสามารถในการตอบสนองที่ดีขึ้นอย่างไรก็ตามได้รับการยอมรับว่า Zero Trust ยังไม่ได้แทนที่ระบบรักษาความมั่นคงปลอดภัยแบบดั้งเดิมอย่างสมบูรณ์

Cybersecurity and Infrastructure Security Agency (2023) ได้ให้ข้อสรุปที่น่าสนใจดังนี้ การดำเนินการตามนโยบายอัตโนมัติ และการจัดการอุปกรณ์ที่ปรับแต่งเป็นสิ่งสำคัญสำหรับการนำไปใช้ความน่าเชื่อถือเป็นศูนย์กลางมีประสิทธิภาพความทันสมัยของความมั่นคงปลอดภัยทางไซเบอร์ต้องใช้แนวทางที่ประสานงาน และทำงานร่วมกันโดยมีการซื้อขายทั่วทั้งหน่วยงานสำหรับสถาปัตยกรรม และนโยบายการกำกับดูแลร่วมกัน การมีส่วนร่วมของผู้มีส่วนได้ส่วนได้เสียรวมถึงผู้บริหารอาวุโส พนักงานไอที เจ้าของข้อมูลและระบบ และผู้ใช้เป็นสิ่งจำเป็น ข้อควรพิจารณา เช่น ข้อมูลรับรอง การประเมินห่วงโซ่อุปทาน และการเปลี่ยนแปลงของเกณฑ์ความเสี่ยง เมื่อใช้แบบจำลองความมั่นคงปลอดภัยที่ไม่มีความน่าเชื่อถือ

2.11 สรุป

บทที่ 2 เป็นการเสนอแนวคิดและทฤษฎีที่เกี่ยวข้อง ตามที่ได้กล่าวมานั้น ผู้วิจัยมุ่งเน้นการพัฒนา ระบบป้องกันเครื่องคอมพิวเตอร์แม่ข่ายแบบเรียลไทม์ รวมถึงมีการแจ้งเตือนให้ผู้ดูแลระบบได้ทราบถึงภัยคุกคามที่เกิดขึ้นได้ทันเหตุการณ์ โดยใช้เทคนิคการวิเคราะห์จากกิจกรรมที่เกิดกับเครื่องคอมพิวเตอร์แม่ข่าย ด้วย MITRE ATT&CK Framework และเปรียบเทียบกับแนวทางการป้องกันการโจมตีเพื่อให้เกิดความมั่นคงปลอดภัยได้ ฉะนั้นการใช้แนวทาง Zero Trust Architecture มาปรับปรุงการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย และทำให้เกิดความมีประสิทธิภาพการป้องกันในเชิงนโยบายมากขึ้นตามไปด้วย

ผู้วิจัยเข้าใจแนวความคิด และทฤษฎีเพื่อนำไปปรับใช้ในการเน้นบทบาทของ SIEM ในการปรับปรุงการทำงานด้านความมั่นคงปลอดภัยโดยการจัดหาแดชบอร์ดส่วนกลางสำหรับการวิเคราะห์บันทึกการแจ้งเตือน และการแจ้งเตือน ด้วยเทคนิค MITRE ATT&CK ในการปรับปรุงการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์เน้นความจำเป็นในการตรวจสอบแบบเรียลไทม์ การคัดกรองภัยคุกคาม และการตรวจจับและตอบสนองภัยคุกคามที่มีประสิทธิภาพ

บทที่ 3

วิธีดำเนินการวิจัย

ผู้วิจัยได้วางแนวทางการพัฒนาระบบป้องกันโจมตีระบบเรียลไทม์ โดยอาศัยหลักการทำงานของระบบ SIEM และการคัดกรองวิเคราะห์การโจมตีโดยหลักการของ MINTER ATT&CK เพื่อให้เกิดความเข้าใจในรายละเอียดของแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง ผู้วิจัยได้กำหนดขั้นตอนการดำเนินงานตามแนวทางวงจรพัฒนาระบบ (System Development Life Cycle : SDLC) โดยมีทั้ง 8 ขั้นตอน ดังนี้

- 3.1 ขั้นตอนการดำเนินงานวิจัย
- 3.2 เครื่องมือใช้ในการวิจัย
- 3.3 ออกแบบ และพัฒนาการตอบสนองการโจมตี และการแจ้งเตือน
- 3.4 ทดสอบการป้องกันการโจมตีและการแจ้งเตือน
- 3.5 ระยะเวลาในการดำเนินงาน
- 3.6 การประเมินประสิทธิภาพการโจมตีแบบเรียลไทม์ และแจ้งเตือน
- 3.7 ข้อจำกัดของงานวิจัย
- 3.8 สรุป

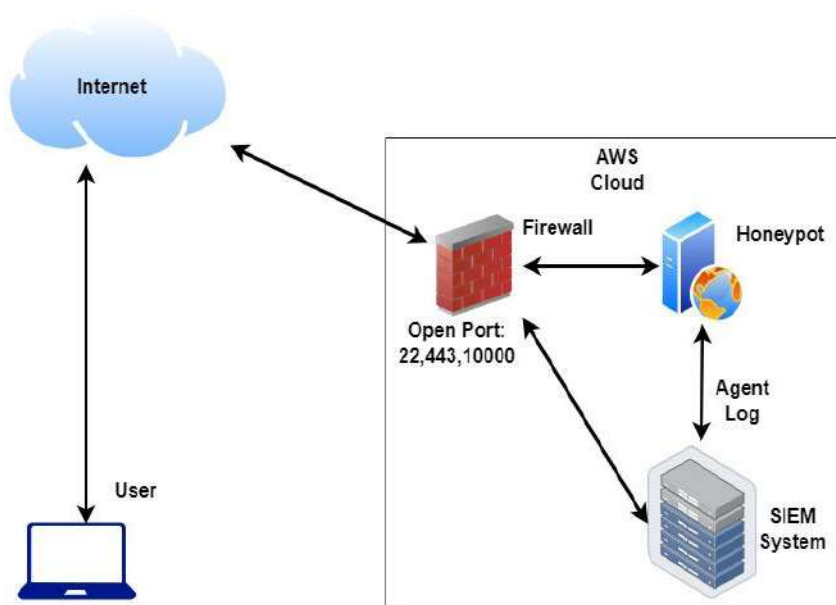
3.1 ขั้นตอนการดำเนินงานวิจัย

ผู้วิจัยได้แบ่งขั้นตอนการวิจัยออกเป็นทั้งหมด 4 ขั้นตอน ซึ่งเป็นขั้นตอนการนำ หลักการ SDLC มาปรับใช้ให้สอดคล้องกับการวิจัย และเพื่อความชัดเจนถึงขั้นตอนการดำเนินงานที่เป็นแบบแผน เพื่อในการพัฒนาตรงตามวัตถุประสงค์ที่กำหนดไว้ในงานวิจัยครั้งนี้

- 3.1.1 การเก็บรวบรวมข้อมูลการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายผ่านการใช้ SSH และ Web Portal

การจัดเก็บระบบ Log System จากเครื่องคอมพิวเตอร์แม่ข่ายซึ่งมีการใช้ในปัจจุบันนั้น สามารถทำได้โดยการกำหนดค่าการจะส่งจากเครื่องคอมพิวเตอร์แม่ข่ายโดยตรงมายังที่จัดเก็บ Log System นั้นมีการจัดเตรียมไว้

(Sina Gholamian, Paul A. S. Ward, 2021) ได้อธิบายว่า Logging system คือระบบที่ใช้ในการบันทึกข้อมูลเวลาทำงานของระบบซอฟต์แวร์ เช่น เวลาเกิดเหตุการณ์ ความสำคัญของเหตุการณ์ และข้อมูลอื่นๆ เพื่อให้ นักพัฒนาและผู้ดูแลระบบสามารถตรวจสอบพฤติกรรมของระบบและวิเคราะห์ข้อมูลได้ในสภาวะการใช้งานจริง ซึ่งเราสามารถรวบรวม และวิเคราะห์ระบบต่างๆ มีความสามารถในการโจมตีได้มีประสิทธิภาพ โดยผู้ดูแลระบบและนักพัฒนาสามารถตรวจสอบพฤติกรรมของระบบ ติดตามปัญหา วิเคราะห์ข้อมูลที่บันทึก ตรวจสอบ และวินิจฉัย ความล้มเหลว เพื่อปรับปรุงความปลอดภัย และเพิ่มประสิทธิภาพการทำงาน รายละเอียดดังประกอบที่ 3.1



ภาพประกอบที่ 3.1 แสดง การจัดเก็บ Log ระบบ SIEM System

การจัดเก็บ Log ระบบ SIEM Open Source ของ Wazuh (Wazuh Inc.h, 2023) ได้ทำอธิบายตามกระบวนการขั้นตอนต่างๆ ดังนี้

1. สร้างเครื่องคอมพิวเตอร์แม่ข่าย โดย Centos7 และ Website ของบริษัทไอทีจำลอง รวมถึงจดโดเมนเพื่อให้เกิดความสมจริง ในการใช้เป็นเหยื่อล่อ เพื่อเก็บค่าการโจมตีเครื่องคอมพิวเตอร์แม่ข่าย หรือเรียกว่า Honeypot ดังภาพประกอบที่ 3.2 โดย Honeypot (Honeypots: Tracking Hackers, 2022) ถือ

กำเนิดในปี 1999 โดย Lance Spitzner ซึ่งมีการติดตั้งระบบเพื่อใช้ลวงให้ผู้บุกรุกเข้ามาโจมตีระบบ เพื่อใช้เป็นวิธีการศึกษาการโจมตีใหม่ๆ ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้เป็นเหยื่อล่อ นั้น ๆ



ภาพประกอบที่ 3.2 แสดงเครื่องคอมพิวเตอร์แม่ข่ายใช้เป็น Honeypot

2. กระบวนการ Log Collector โดยการติดตั้งโปรแกรมเสริม (Agent) ที่เครื่องคอมพิวเตอร์แม่ข่ายที่เป็นตัวเหยื่อล่อ (Honeypot) เพื่อรวบรวมบันทึกเหตุการณ์จากจุดสิ้นสุด แอปพลิเคชัน และอุปกรณ์เครือข่ายที่ได้รับการตรวจสอบดังภาพ ภาพประกอบที่ 3.3

```

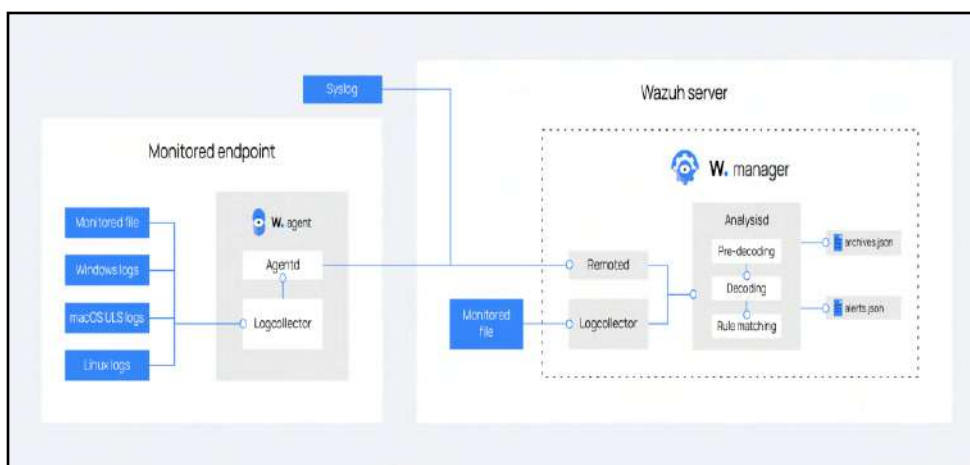
wazuh-agent.service - Wazuh agent
Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; enabled; vendor preset: disabled)
Active: active (running) since Sat 2024-06-15 17:36:47 +07; 1 weeks 1 days ago
Tasks: 30
CGroup: /system.slice/wazuh-agent.service
├─1138 /var/ossec/bin/wazuh-execd
├─1180 /var/ossec/bin/wazuh-agentd
├─1199 /var/ossec/bin/wazuh-syscheckd
├─1223 /var/ossec/bin/wazuh-logcollector
└─1271 /var/ossec/bin/wazuh-modulesd

Jun 15 17:36:39 ip-172-31-45-16.ap-southeast-1.compute.internal systemd[1]: Starting Wazuh agent...
Jun 15 17:36:39 ip-172-31-45-16.ap-southeast-1.compute.internal env[1081]: Starting Wazuh v4.5.4...
Jun 15 17:36:41 ip-172-31-45-16.ap-southeast-1.compute.internal env[1081]: Started wazuh-execd...
Jun 15 17:36:42 ip-172-31-45-16.ap-southeast-1.compute.internal env[1081]: Started wazuh-agentd...
Jun 15 17:36:43 ip-172-31-45-16.ap-southeast-1.compute.internal env[1081]: Started wazuh-syscheckd...
Jun 15 17:36:44 ip-172-31-45-16.ap-southeast-1.compute.internal env[1081]: Started wazuh-logcollector...
Jun 15 17:36:45 ip-172-31-45-16.ap-southeast-1.compute.internal env[1081]: Started wazuh-modulesd...
Jun 15 17:36:47 ip-172-31-45-16.ap-southeast-1.compute.internal env[1081]: Completed.
Jun 15 17:36:47 ip-172-31-45-16.ap-southeast-1.compute.internal systemd[1]: Started Wazuh agent.
root@ip-172-31-45-16 ~]#

```

ภาพประกอบที่ 3.3 แสดงสถานะการทำงาน Agent บน Honeypot

3. เซิร์ฟเวอร์ Wazuh จะรับค่าบันทึกเหตุการณ์ต่างๆที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่าย มาทำการวิเคราะห์กับตัวแปรของ MITRE ATT&CK Framework ที่บันทึกที่รวบรวมไว้แบบเรียลไทม์โดยใช้ตัวถอดรหัส และกฎเงื่อนไข Wazuh ดึงข้อมูลที่เกี่ยวข้องจากบันทึก และจับคู่ลงในฟิลด์ข้อมูลที่เหมาะสมโดยใช้ตัวถอดรหัส สำหรับโมดูลการวิเคราะห์ในเซิร์ฟเวอร์ Wazuh จะประเมินบันทึกที่ถอดรหัสตามกฎเงื่อนไขที่กำหนดค่าไว้ และทำการบันทึกการแจ้งเตือนในไฟล์แจ้งเตือน ดังภาพประกอบที่ 3.4

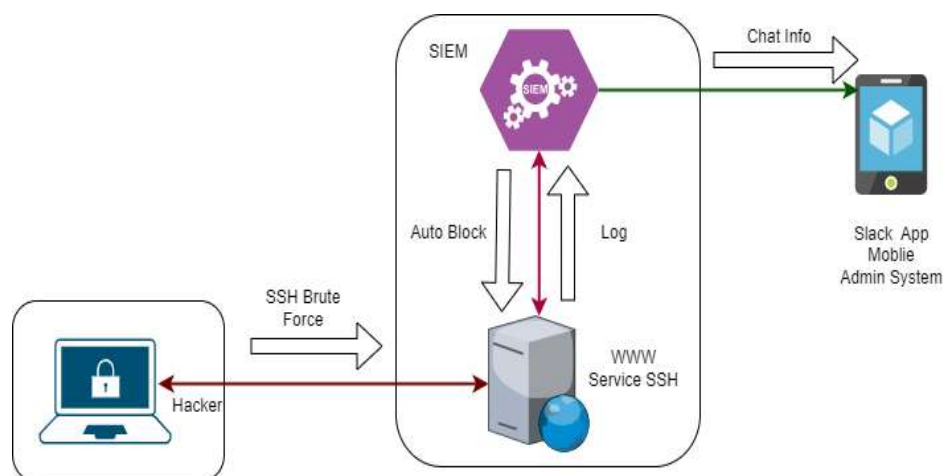


ภาพประกอบที่ 3.4 แสดงการส่งค่า Log ระหว่าง Agent กับ SIEM

ที่มา : Wazuh.com, 2566

นอกเหนือจากบันทึกการแจ้งเตือนแล้วยังจัดเก็บบันทึกที่รวบรวมไว้ทั้งหมดในไฟล์บันทึกการเก็บถาวรที่ไฟล์ Archives ไฟล์บันทึกการเก็บถาวรเหล่านี้จะบันทึกทั้งหมดอย่างครอบคลุม รวมถึงที่ไม่ทำให้เกิดการแจ้งเตือนใดๆ คุณลักษณะนี้ช่วยให้มั่นใจได้ถึงบันทึกที่ครอบคลุมของกิจกรรมของระบบทั้งหมดสำหรับการอ้างอิง และการวิเคราะห์ในอนาคตได้

อย่างไรก็ดี เซิร์ฟเวอร์จะเก็บบันทึก และจะไม่ลบออกโดยอัตโนมัติ แต่คุณสามารถเลือกเวลาที่ลบบันทึกเหล่านี้ด้วยตนเองหรือโดยอัตโนมัติตามข้อกำหนดทางกฎหมายและข้อบังคับ รายละเอียดดังประกอบที่ 3.5



ภาพประกอบที่ 3.5 แสดง SIEM Flow System

3.1.2 กำหนดเงื่อนไขการตอบสนองเมื่อมีการโจมตีและการแจ้งเตือน

จากการบันทึก Log System ที่ได้ทำการจัดเก็บจากเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้ Agent นำส่งค่าที่อยู่ในระบบ Log System ส่งข้อมูลผ่าน API มาที่ระบบ SIEM ของ Wazuh จะทำการกำหนดค่าพารามิเตอร์ต่างๆในรูปแบบค่า Json ให้มาเป็นตาราง Table รายละเอียดดังประกอบที่ 3.6

```
{
  "_index": "wazuh-alerts-4.x-2023.11.10",
  "_id": "4VNLuYaBbPLCgt_Dg9CY",
  "_version": 1,
  "_score": null,
  "_source": {
    "predecoder": {
      "hostname": "ip-172-31-45-16",
      "program_name": "sshd",
      "timestamp": "Nov 10 14:03:22"
    },
    "input": {
      "type": "log"
    },
    "agent": {
      "ip": "172.31.45.16",
      "name": "WWW",
      "id": "003"
    },
    "data": {
      "srcuser": "deployer",
      "srcip": "82.156.171.245"
    }
  }
}
```

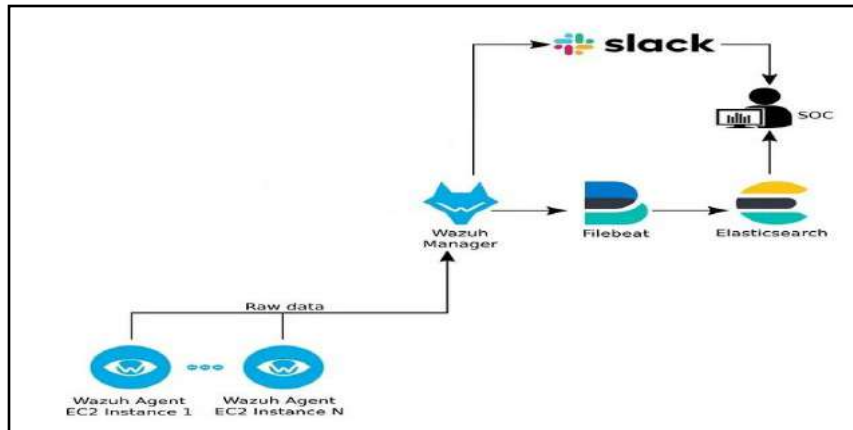
ภาพประกอบที่ 3.6 แสดงบันทึก Log System จาก Agent

ใช้การเปรียบเทียบค่าต่างๆ ที่ได้นั้นนำไปเปลี่ยนการค่ากำหนดในข้อกำหนด MITRE ATT&CK Framework เพื่อทำการเปรียบเทียบเงื่อนไขที่อยู่ข้อกำหนดของ MITRE ATT&CK Framework และทำการ Comment ไปในค่าการแจ้งเตือน ว่าเป็นการโจมตีหรือไม่ และเป็นกิจกรรมอะไรกระบวนการใด เพื่อใช้ในการวิเคราะห์ รายละเอียดดังประกอบที่ 3.7

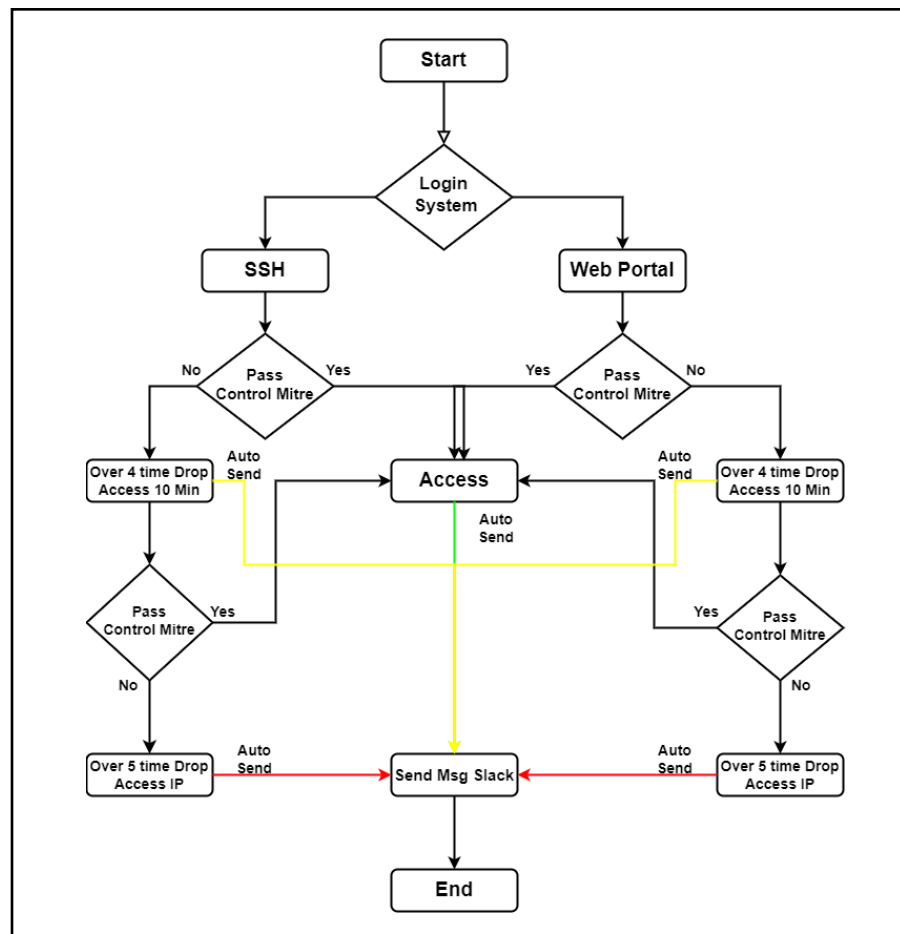
rule.gdpr	IV.35.7.d, IV.32.2
rule.gpg13	7.1
rule.groups	syslog, sshd, authentication_failed, invalid_login
rule.hipaa	164.312.b
rule.id	5710
rule.level	5
rule.mail	false
rule.mitre.id	T1110.001, T1021.004
rule.mitre.tactic	Credential Access, Lateral Movement
rule.mitre.technique	Password Guessing, SSH
rule.nist_800_53	AU.14, AC.7, AU.6
rule.pci_dss	10.2.4, 10.2.5, 10.6.1
rule.tsc	CC6.1, CC6.8, CC7.2, CC7.3
timestamp	Nov 10, 2023 @ 21:03:23.563

ภาพประกอบที่ 3.7 แสดงค่าเปรียบเทียบของ MITRE ATT&CK Framework

การตั้งเงื่อนไขเพื่อหยุดการโจมตีได้แบบเรียลไทม์หรือการแจ้งเตือน ฉะนั้นค่าต่างๆ ผู้ทำวิจัยจึงต้องนำมาวิเคราะห์ และเปรียบเทียบกับ กระบวนการป้องกัน เพื่อหยุดการโจมตี SSH Brute Force ที่เกิดขึ้นกับแม่ข่าย และอีกทั้งต้องใช้ค่ากิจกรรมที่เกิดขึ้นแบบไม่ปกติจากการโจมตี นำไปเป็นกฎเงื่อนไขที่ใช้ในการแจ้งเตือนไปยัง Slack เพื่อเตือนให้ผู้ดูแลระบบทราบว่ามีการโจมตี เครื่องคอมพิวเตอร์แม่ข่ายในขณะนั้น เพื่อใช้ในการกำหนดการเชื่อมต่อ รายละเอียดดังประกอบที่ 3.8 ถึง 3.9



ภาพประกอบที่ 3.8 แสดง การเชื่อมต่อระหว่างระบบของ SIEM



ภาพประกอบที่ 3.9 แสดงเงื่อนไขการป้องกัน Brute Force แบบเรียลไทม์

3.1.3 เงื่อนไขการตอบสนองปรับใช้ตามจุดประสงค์งานวิจัย

การนำเงื่อนไขของการเปรียบเทียบค่าใน Log Even มาทำการหาแนวทางการป้องกันโดยหลักการจากใช้เครื่องมือการโจมตี หรือแนวทางการโจมตีมาใช้ในการวิเคราะห์แนวทางการป้องกันว่าขั้นตอนทำป้องกันมีที่ระดับ จากนั้นนำเงื่อนไขมาปรับใช้กับเงื่อนไข เพื่อให้เป็นไปตามที่ผู้วิจัยกำหนด ดังตามรูปภาพประกอบที่ 3.5 แสดงเงื่อนไขการป้องกัน Brute Force แบบเรียลไทม์

จากกระบวนการเงื่อนไขนี้สามารถนำไปปรับใช้การตั้งเงื่อนไขในระบบ SIEM เพื่อให้ตอบสนองตรงตามเงื่อนไขที่ได้กำหนด จากนั้น นำไปทดสอบการใช้งานอีกครั้ง เพื่อดูผลการป้องกัน หากผลยังไม่ตรงจุดประสงค์การวิจัย ต้องปรับพัฒนาเงื่อนไขให้สอดคล้องอีกครั้งจนได้ตรงตามจุดประสงค์

3.1.4 รวมผลการทดสอบการป้องกันเครื่องคอมพิวเตอร์แม่ข่ายแบบเรียลไทม์ ในรูปแบบต่างๆ

เมื่อการตั้งเงื่อนไขเรียบร้อยแล้วเป็นการทดสอบการการป้องกันโดยกำหนดตัวชี้วัดจากจำนวนที่การป้องกัน กับเครื่องมือ ต่างๆ ที่ใช้ในการ Brute Force ว่าสามารถใช้ในการป้องกันแบบเรียลไทม์หรือไม่โดยเครื่องมือที่ใช้จำนวน 3 รูปแบบ แต่ละแบบใช้ในการทดสอบจำนวน 5 ครั้ง ตามภาพประกอบที่

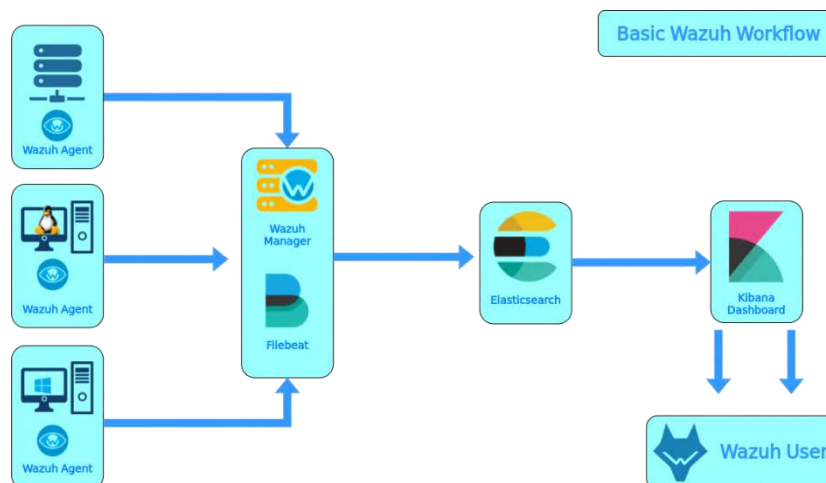
3.9 แสดงค่าใช้ในการชี้วัดการทดสอบ SSH Brute Force

3.2 เครื่องมือใช้ในการวิจัย

ในงานวิจัยนี้ ได้นำเครื่องมือต่าง ๆ เพื่อมาใช้ในการวิจัยการป้องกันเครื่องคอมพิวเตอร์แม่ข่ายแบบเรียลไทม์ โดยเครื่องมือนี้เป็น Open Source นำไปประยุกต์ใช้ได้มากมาย และรวมถึงการพัฒนาต่อยอดในเชิงธุรกิจ และไม่ติดปัญหาเรื่อง License สำหรับใช้ในเชิงพาณิชย์ หรือ หน่วยงานราชการ

3.2.1 ระบบ SIEM Open Source (Wazuh)

Wazuh เป็นแพลตฟอร์มรักษาความปลอดภัยโอเพ่นซอร์สฟรีที่มีความสามารถ SIEM แพลตฟอร์มนี้นำเสนอการวิเคราะห์ข้อมูลบันทึก การตรวจจับการบุกรุก และมัลแวร์ การตรวจสอบความสมบูรณ์ของไฟล์ การประเมินการกำหนดค่า การตรวจจับช่องโหว่ การสนับสนุนการปฏิบัติตามกฎระเบียบ และการตอบสนองที่ใช้งานอยู่ด้วย Wazuh ผู้ใช้สามารถในสภาพแวดล้อมแบบ On-Premises, Virtualized, Containerized และระบบคลาวด์ได้ Wazuh ประกอบด้วยองค์ประกอบหลักสามส่วนและเอเจนต์ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายที่อเนกประสงค์ ตามภาพประกอบที่ 3.10



ภาพประกอบที่ 3.10 แสดง Basic Wazuh Workflow

ที่มา : Github.com, 2566

1. องค์ประกอบส่วนกลางของ Wazuh (เซิร์ฟเวอร์ ตัวสร้างดัชนี และแดชบอร์ด) วิเคราะห์ข้อมูลความปลอดภัยที่รวบรวมจากเอเจนต์ สามารถกำหนดค่าได้ภายในองค์กรได้ เอเจนต์ถูกปรับใช้บนเครื่องคอมพิวเตอร์แม่ข่ายที่ได้รับการตรวจสอบเพื่อรวบรวมข้อมูล และตอบสนองต่อภัยคุกคาม

Wazuh ใช้แหล่งข่าวกรองภัยคุกคามเพื่อปรับปรุงความสามารถในการตรวจจับ นอกจากนี้ยังเสริมข้อมูลการแจ้งเตือนโดยใช้กรอบงาน MITER ATT&CK และข้อกำหนดการปฏิบัติตามกฎระเบียบ เช่น PCI DSS, GDPR, HIPAA, CIS และ NIST 800-53 สำหรับการวิเคราะห์ความปลอดภัย

2. กระบวนการจัดเก็บ Log System กระบวนการนี้ดำเนินการโดยเอเจนต์ที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายซึ่งสามารถอ่านไฟล์บันทึกและกิจกรรมบน Windows โดยการรวบรวมของระบบปฏิบัติการและข้อความบันทึกของแอปพลิเคชัน รองรับตัวกรอง XPath สำหรับ Windows และจัดจํารูปแบบหลายบรรทัด เช่น บันทึกการตรวจสอบระบบปฏิบัติการ Linux โดยรวบรวมเอาต์พุตและรายงานกลับไปยังเซิร์ฟเวอร์ Wazuh เพื่อการวิเคราะห์เพิ่มเติม คุณสามารถใช้โมดูลนี้เพื่อจุดประสงค์ที่แตกต่างกัน เช่น การตรวจสอบพื้นที่ว่างบนฮาร์ดดิสก์หรือการรับรายชื่อผู้ใช้ที่เข้าสู่ระบบครั้งล่าสุด รายละเอียดดังประกอบที่ 3.11

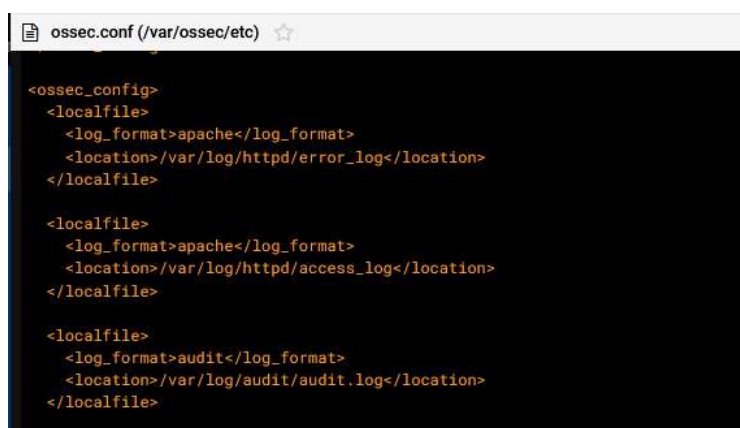
```

    },
    "agent": {
      "ip": "172.31.45.16",
      "name": "WWW",
      "id": "003"
    },
    "previous_output": "58.11.20.19 - root [23/Jun/2024:21:56:53 +0700] \"POST /extensions/
file-manager/tree.cgi?module=filemin&d=3 HTTP/1.1\" 200 60\n58.11.20.19 - root [23/Jun/202
4:21:56:50 +0700] \"POST /extensions/file-manager/list.cgi?module=filemin&page=1&paginate=1
4&overwrite_efiles=false&follow_symlinks=false HTTP/1.1\" 200 20447\n58.11.20.19 - root [2
3/Jun/2024:21:56:50 +0700] \"POST /extensions/file-manager/tree.cgi?module=filemin&d=3 HTT
P/1.1\" 200 2447\n58.11.20.19 - root [23/Jun/2024:21:56:45 +0700] \"POST /extensions/file-m
anager/list.cgi?module=filemin&page=1&paginate=14&overwrite_efiles=false&follow_symlinks=fa
lse HTTP/1.1\" 200 36630\n58.11.20.19 - root [23/Jun/2024:21:56:45 +0700] \"POST /extension
s/file-manager/tree.cgi?module=filemin&d=3 HTTP/1.1\" 200 18965\n58.11.20.19 - root [23/Ju
n/2024:21:56:35 +0700] \"POST /extensions/file-manager/tree.cgi?module=filemin&d=3&y=1&e=1
HTTP/1.1\" 200 149582\n58.11.20.19 - root [23/Jun/2024:21:56:34 +0700] \"POST /extensions/f
ile-manager/list.cgi?module=filemin&page=1&paginate=9&overwrite_efiles=false&follow_symlink
s=false HTTP/1.1\" 200 31820";

```

ภาพประกอบที่ 3.11 แสดง Log System ที่ทำการเก็บบันทึก

Agent ได้มีการติดตั้งลงเครื่องคอมพิวเตอร์แม่ข่ายเรียบร้อยแล้วจากนั้นทำการตั้งค่าพารามิเตอร์ได้ระบุที่อยู่ของไฟล์ Log System ของเครื่องคอมพิวเตอร์แม่ข่าย โมดูลตัวแทนทั้งหมดสามารถกำหนดค่าได้ และทำงานด้านความปลอดภัยที่แตกต่างกัน สถาปัตยกรรมแบบโมดูลาร์ นี้ช่วยให้คุณสามารถเปิดหรือปิดใช้งานแต่ละส่วนประกอบได้ตามความต้องการด้านความปลอดภัยของคุณ ด้านล่างนี้ คุณสามารถเรียนรู้เกี่ยวกับวัตถุประสงค์ที่แตกต่างกันของโมดูลตัวแทนทั้งหมดได้ รายละเอียดดังประกอบที่ 3.12



```

ossec.conf (/var/ossec/etc) ☆
<ossec_config>
  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/httpd/error_log</location>
  </localfile>

  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/httpd/access_log</location>
  </localfile>

  <localfile>
    <log_format>audit</log_format>
    <location>/var/log/audit/audit.log</location>
  </localfile>

```

ภาพประกอบที่ 3.12 แสดงตัวอย่างการจัดเก็บ Log System CentOS7

3. แดชบอร์ด Wazuh เป็นอินเทอร์เฟซผู้ใช้งานผ่าน Web Application ที่ให้ความยืดหยุ่นและใช้งานง่ายสำหรับการวิเคราะห์ และการแสดงภาพกิจกรรมด้านความปลอดภัย และข้อมูลการแจ้งเตือน นอกจากนี้ยังใช้สำหรับการจัดการ และการตรวจสอบแพลตฟอร์ม Wazuh นอกจากนี้ยังมีคุณสมบัติสำหรับการเข้าใช้งานแบบ Role-Based Access control (RBAC) และ Single Sign-On (SSO)

เว็บอินเทอร์เฟซช่วยให้ผู้ใช้นำทางผ่านข้อมูลประเภทต่างๆ ที่รวบรวมโดยตัวแทน Wazuh รวมถึงการแจ้งเตือนความปลอดภัยที่สร้างโดยเซิร์ฟเวอร์ Wazuh ผู้ใช้ยังสามารถสร้างรายงาน และสร้างการแสดงผล และแดชบอร์ดที่กำหนดเองได้ที่พร้อมใช้งานทันทีสำหรับการปฏิบัติตามกฎระเบียบ เช่น PCI DSS, GDPR, HIPAA และ NIST 800-53 นอกจากนี้ยังมีอินเทอร์เฟซเพื่อนำทางผ่านกรอบงาน MITRE ATT&CK และการแจ้งเตือนที่เกี่ยวข้อง รายละเอียดดังประกอบที่ 3.13

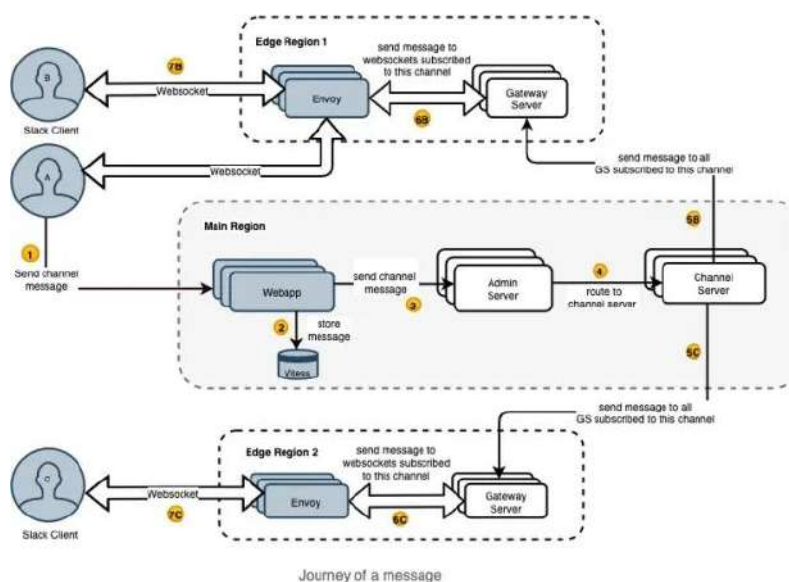


ภาพประกอบที่ 3.13 แสดง แดชบอร์ดอินเทอร์เฟซผู้ใช้งาน

3.2.2 ระบบ Slack สำหรับการแจ้งเตือนผ่าน Application Internet

Slack คือบริการส่งข้อความโต้ตอบแบบทันทีข้ามแพลตฟอร์มแบบฟรีบนคลาวด์ ที่สร้างโดย Slack Technologies และปัจจุบันเป็นของ Salesforce แม้ว่าในตอนแรกจะได้รับการพัฒนาเพื่อการ

สื่อสารระดับมืออาชีพ และระดับองค์กร แต่ก็ถูกนำมาใช้เป็นแพลตฟอร์มชุมชนด้วย ผู้ใช้สามารถสื่อสารผ่านการส่งข้อความ การแชร์ไฟล์และสื่อ การโทรด้วยเสียง และวิดีโอในการแชทส่วนตัวหรือภายในชุมชนที่เรียกว่า “Workspaces” แอปพลิเคชันนี้รวมองค์ประกอบสไลด์ IRC เช่น ห้องสนทนาถาวร (เรียกว่าช่องทาง) ที่จัดเรียงตามหัวข้อ กลุ่มส่วนตัว และการส่งข้อความโดยตรง นอกเหนือจากคุณสมบัติการสื่อสารออนไลน์เหล่านี้แล้ว Slack ยังสามารถทำงานร่วมกับซอฟต์แวร์อื่น ๆ ได้อีกด้วย Slack สามารถเข้าถึงได้ผ่านเว็บเบราว์เซอร์ และมีไคลเอนต์เฉพาะสำหรับ Windows, Linux, MacOS, Android และ iOS รายละเอียดดังประกอบที่ 3.14



ภาพประกอบที่ 3.14 แสดง Data Flow Message

ที่มา : Slack.Engineering, 2566

3.2.3 เครื่องคอมพิวเตอร์แม่ข่าย CentOS 7 และ Webmin เครื่องมือการดูแลระบบบนเว็บสำหรับเซิร์ฟเวอร์

CentOS คือ ระบบปฏิบัติการ Community Enterprise Operating System หรือ ระบบปฏิบัติการ Linux สำหรับองค์กรที่เน้นเรื่องความเสถียร และมีการอัปเดตความปลอดภัยระดับสูง โดยเวอร์ชันใหม่

ประมาณทุก 2 ปี โดยแต่ละเวอร์ชันมีอายุการใช้งานสูงสุด 10 ปี หรือตามข้อกำหนดระยะเวลาการสนับสนุนของ Red Hat Enterprise Linux (RHEL) และในแต่ละเวอร์ชันได้รับการอัปเดตประมาณทุก 6 เดือน ทำให้ระบบ Linux มีความปลอดภัย และมีความน่าเชื่อถือ

CentOS เปิดตัวอย่างเป็นทางการครั้งแรกในปี ค.ศ. 2004 โดย Gregory Kurtze เป็นผู้ก่อตั้ง ซึ่งเป็น Open Source ที่พัฒนามาจากโค้ดต้นฉบับ (Source Code) ของ RedHat Enterprise Linux (RHEL) ระบบปฏิบัติการที่มีความเสถียรรองรับ Workload ที่หลากหลาย สามารถนำไปพัฒนาซอฟต์แวร์ Open Source อื่นๆ ได้ ซึ่งเป็นลิขสิทธิ์แบบ GNU General Public License (GNU-GPL) หมายถึง สัญญาอนุญาตให้นักพัฒนาสามารถใช้ซอฟต์แวร์ รวมถึงสามารถทำซ้ำ เผยแพร่ และดัดแปลงซอฟต์แวร์นั้นได้ เพื่อให้นักพัฒนาทุกคนสามารถใช้งานซอฟต์แวร์ดังกล่าวได้อย่างอิสระ และถูกต้องตามกฎหมาย (Openlandscape.cloud, 2023)

1. CentOS Version ปัจจุบัน CentOS มีระบบปฏิบัติการทั้งหมด 4 เวอร์ชัน ทั้ง CentOS เวอร์ชันเดิม และ CentOS Stream เวอร์ชันใหม่ โดยคุณยังสามารถเลือกใช้งาน CentOS เวอร์ชันเก่าได้ แต่อาจมีข้อจำกัดบางอย่างเมื่อเทียบกับ CentOS เวอร์ชันรุ่นที่ใหม่กว่า เนื่องจากมีการปรับปรุงข้อบกพร่องที่พบในเวอร์ชันเก่าให้ดียิ่งขึ้น อีกทั้งยังมีการอัปเดต และการบำรุงรักษาให้ทันสมัยอยู่เสมอ โดยแต่ละเวอร์ชันมีระยะ End of Life รายละเอียดดังประกอบที่ 3.15

CentOS Version มีอะไรบ้าง ?			
รุ่น	วันที่เปิดให้ใช้งาน	อัปเดตเต็มรูปแบบ	อัปเดตและการบำรุงรักษา
3	ค.ศ. 2004 - 03 - 19	ค.ศ. 2006 - 07 - 20	ค.ศ. 2010 - 10 - 31
4	ค.ศ. 2005 - 03 - 09	ค.ศ. 2009 - 03 - 31	ค.ศ. 2012 - 02 - 29
5	ค.ศ. 2007 - 04 - 12	ค.ศ. 2014 - 01 - 31	ค.ศ. 2017 - 03 - 31
6	ค.ศ. 2011 - 07 - 10	ค.ศ. 2017 - 05 - 10	ค.ศ. 2020 - 11 - 30
7	ค.ศ. 2014 - 07 - 07	ค.ศ. 2020 - 08 - 06	ค.ศ. 2024 - 06 - 30
8	ค.ศ. 2019 - 09 - 24	ค.ศ. 2021 - 12 - 31	-
9	ค.ศ. 2021 - 04 - 26	ค.ศ. 2027	-

● CentOS เวอร์ชันเก่า
● CentOS เวอร์ชันเดิมที่รองรับการอัปเดต
● CentOS เวอร์ชันเดิมล่าสุด
● CentOS Stream เวอร์ชันใหม่

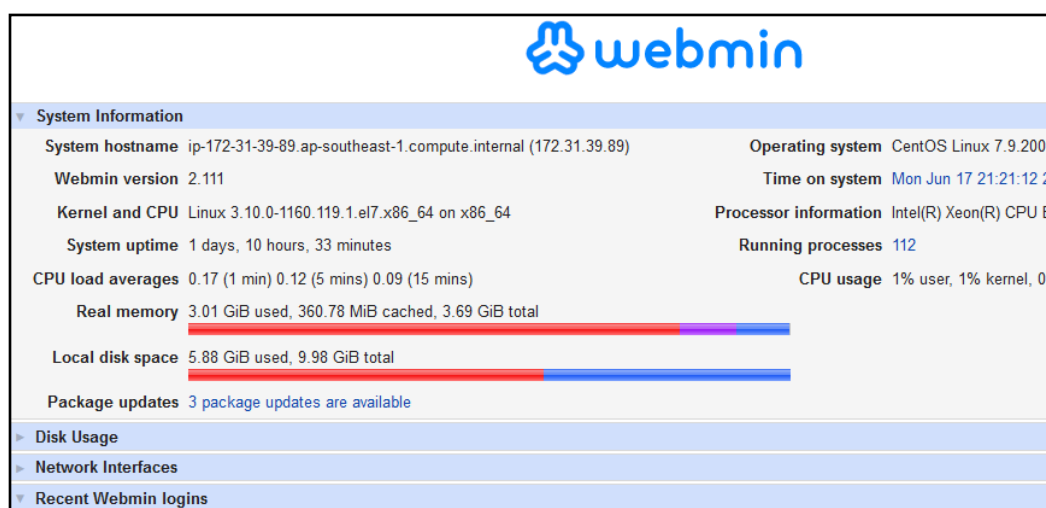
ภาพประกอบที่ 3.15 แสดง CentOS Version

ที่มา : <https://blog.openlandscape.cloud/centos>, 2566

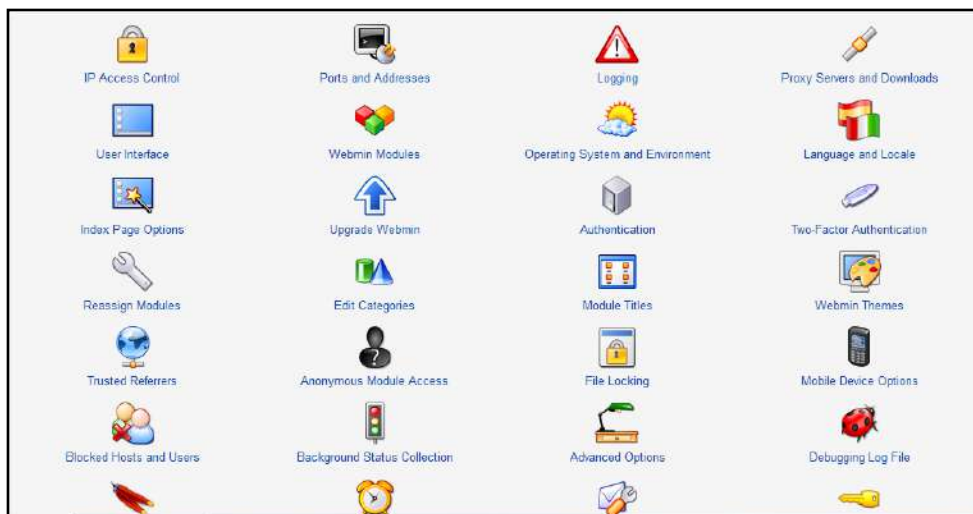
2. ประโยชน์ที่ได้จากการใช้ CentOS

- ใช้งานได้ Free ช่วยประหยัดงบประมาณโดยไม่จำเป็นต้องจ่ายค่าลิขสิทธิ์ซอฟต์แวร์
- มี Package ให้ใช้งานมากมาย CentOS มีแพ็คเกจย่อยที่สามารถนำมาใช้ทำ Server สำหรับใช้งานในองค์กรได้ เช่น Antivirus Server (ClamAV), Control Panel (ISPConfig), Database Server (MySQL / PostgreSQL), DHCP Server (DHCPd), DNS Server (BIND), File and Printer Server (Samba) และ Docker เป็นต้น
- มีการ Update ความปลอดภัยในการใช้งานอยู่เสมอ

Webmin เป็นเครื่องมือการดูแลระบบบนเว็บสำหรับ Linux นอกจากนี้ยังรองรับ UNIX, OS X ที่แกนกลาง Webmin เป็นกระบวนการที่จัดทำรอบงานสำหรับโมดูลเหล่านั้นก็นำเสนอ GUI บนเว็บสำหรับการกำหนดค่า และการโต้ตอบกับ โมดูลที่ทำงานบนเซิร์ฟเวอร์พื้นฐาน โมดูลยังสามารถใช้เพื่อโต้ตอบกับการจัดการผู้ใช้งานโดยต้องการควบคุม Webmin มาพร้อมกับโมดูลในตัวจำนวนมากที่สามารถจัดการงานเซิร์ฟเวอร์ทั่วไปที่มีให้เลือกมากมาย โครงสร้างพื้นฐานเป็นแบบที่ยังสามารถเขียนโมดูลของตนเองหรือดาวน์โหลดโมดูลที่สนับสนุนของการอนุญาต Root ของ Webmin โมดูลของบุคคลที่สามอาจเป็นที่ไม่ปลอดภัย ดังนั้นจึงไม่ควรติดตั้งโมดูลเหล่านี้โดยไม่ได้ตรวจสอบก่อนติดตั้งเพื่อแสดงรายละเอียดต่างๆ รายละเอียดดังภาพประกอบที่ 3.16 และ 3.17



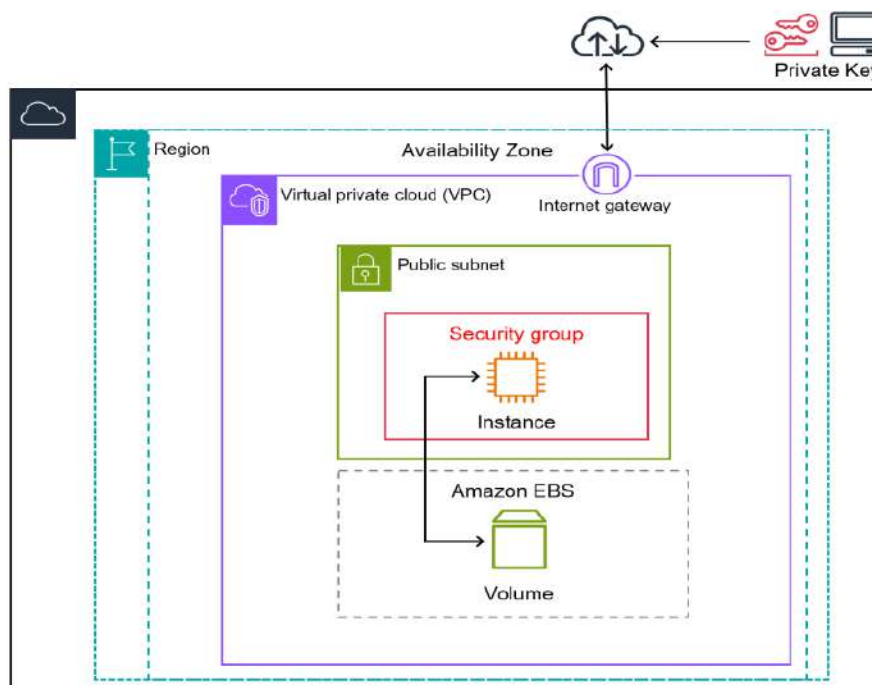
ภาพประกอบที่ 3.16 แสดง รายละเอียด CentOS Version



ภาพประกอบที่ 3.17 แสดง Webmin Configuration

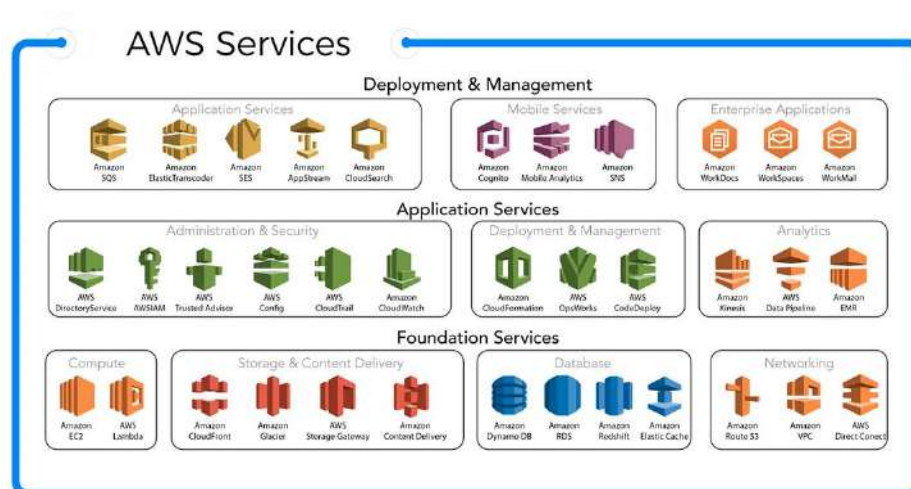
3.2.4 Amazon Elastic Compute Cloud (Amazon EC2) คือบริการให้เช่าระบบการประมวลผลตามความต้องการ และปรับขนาดได้ใน Amazon Web Services (AWS) Cloud การใช้ Amazon EC2 ช่วยลดต้นทุนด้านฮาร์ดแวร์ สามารถพัฒนา และปรับใช้แอปพลิเคชันได้เร็วขึ้น คุณสามารถใช้ Amazon EC2 เพื่อเปิดใช้เซิร์ฟเวอร์เสมือนได้มากหรือน้อยเท่าที่ต้องการ กำหนดค่าความปลอดภัย เครือข่าย และจัดการพื้นที่จัดเก็บข้อมูล คุณสามารถเพิ่มความจุ (ขยายขนาด) เพื่อจัดการกับงานที่ต้องใช้การประมวลผลอย่างหนัก เช่น กระบวนการรายเดือนหรือรายปี หรือปริมาณการเข้าชมเว็บไซต์ที่เพิ่มขึ้นอย่างรวดเร็ว เมื่อการใช้งานลดลง คุณสามารถลดความจุ (ลดขนาด) อีกครั้งได้

ภาพประกอบที่ 3.18 แสดงสถาปัตยกรรมพื้นฐานของ Amazon EC2 instance ที่ใช้งานภายใน Amazon Virtual Private Cloud (VPC) ในตัวอย่างนี้ EC2 instance อยู่ภายใน Availability Zone ในภูมิภาค อินสแตนซ์ EC2 ได้รับการรักษาความปลอดภัยด้วยกลุ่มความปลอดภัย ซึ่งเป็นไฟร์วอลล์เสมือนที่ควบคุมการรับส่งข้อมูลขาเข้า และขาออก รหัสส่วนตัวจะถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์ และรหัสสาธารณะจะถูกเก็บไว้ในอินสแตนซ์ ทั้งสองถูกระบุเป็นคู่คีย์เพื่อพิสูจน์ตัวตนของผู้ใช้ ในสถานการณ์นี้ อินสแตนซ์ได้รับการสนับสนุนโดยวอลุ่ม Amazon EBS VPC สื่อสารกับอินเทอร์เน็ตโดยใช้เกตเวย์อินเทอร์เน็ต สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ Amazon VPC ([docs.aws.amazon.com](https://docs.aws.amazon.com/vpc/latest/userguide/), 2023) รายละเอียดดังภาพประกอบที่ 3.19



ภาพประกอบที่ 3.18 แสดง Basic architecture of an Amazon EC2

ที่มา : Aws.amazon.com , 2566



ภาพประกอบที่ 3.19 แสดง Amazon EC2 Service

ที่มา : aws.amazon.com, 2566

3.2.5 Kali Linux เครื่องมือทดสอบ Brute Force Attack (เดิมชื่อ Back Track Linux, 2013) เป็นระบบปฏิบัติการ Linux แบบโอเพ่นซอร์สที่ใช้ Debian ซึ่งมุ่งเป้าไปที่การทดสอบการเจาะข้อมูลขั้นสูงและการตรวจสอบความปลอดภัย การกำหนดค่า และระบบอัตโนมัติที่ช่วยให้ผู้ใช้สามารถมุ่งเน้นไปที่งานที่ต้องทำให้เสร็จ Kali Linux มีการดัดแปลงเฉพาะอุตสาหกรรม รวมถึงเครื่องมือหลายร้อยรายการที่มุ่งเป้าไปที่งานด้านความปลอดภัยของข้อมูลต่างๆ เช่น การทดสอบการเจาะข้อมูล การวิจัยความปลอดภัย นิติคอมพิวเตอร์ วิศวกรรมย้อนกลับ การจัดการช่องโหว่ และการทดสอบทีมแดง

Kali Linux เป็นโซลูชันหลายแพลตฟอร์ม เข้าถึงได้และใช้งานได้ฟรีสำหรับผู้เชี่ยวชาญด้านความปลอดภัยของข้อมูล (Kali Linux, 2023) รายละเอียดดังภาพประกอบที่ 3.20 และ 3.21

Date	Project Released	Base OS
2004-August-30	Whopper v2	Knoppix
2005-july-17	WHAX v3	Slix
2006-May-26	BackTrack v1	Slackware Live CD 10.2.0
2007-March-06	BackTrack v2	Slackware Live CD 11.0.0
2008-June-19	BackTrack v3	Slackware Live CD 12.0.0
2010-January-09	BackTrack v4 (Pwnsauce)	Ubuntu 8.10 (Intrepid Bebe)
2011-May-10	BackTrack v5 (Revolution)	Ubuntu 10.04 (Lucid Lynx)
2013-March-13	Kali Linux v1 (Moto)	Debian 7 (Wheezy)
2015-August-11	Kali Linux v2 (Seren)	Debian 8 (Jessie)
2016-January-16	Kali Linux rolling	Debian Testing

ภาพประกอบที่ 3.20 แสดง Kali Linux Timeline

ที่มา : Kali Linux, 2023

```

hydra Usage Example

Attempt to login as the root user (-L root) using a password list (-P /usr/share/wordlists/metasploit/unix_passwords.txt) with 6 threads (-t 6) on the given SSH server (ssh://192.168.1.100):

root@kali:~# hydra -L root -P /usr/share/wordlists/metasploit/unix_passwords.txt -t 6 ssh
Hydra v2.11.3 (c)2013 by van Hauser/Hack & David Maciejak - for legal purposes only

Hydra (http://www.vse.org/the-hydra) starting at 2023-07-16 07:13:11
[DATA] 6 tasks, 1 server, 100 login tries (1:1/servers), 1000 tries per task
[DATA] attacking service ssh on port 22

pw-inspector Usage Example

Read in a list of passwords (-F /usr/share/wordlists/rockyou.txt) and save to a file (-o /root/pwinspect.txt), selecting passwords of a minimum length of 6 (-m 6) and a maximum length of 10 (-M 10):

root@kali:~# pw-inspector -F /usr/share/wordlists/rockyou.txt -o /root/pwinspect.txt -m 6 -M 10
root@kali:~# cat /usr/share/wordlists/rockyou.txt
root@kali:~# cat /root/pwinspect.txt
root@kali:~# cat /root/pwinspect.txt

```

ภาพประกอบที่ 3.21 แสดง เครื่องมือที่ใช้โจมตี Password

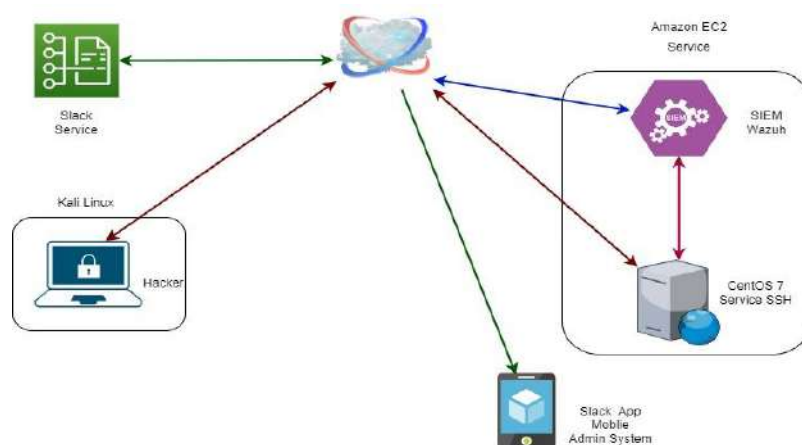
ที่มา : Kali Linux, 2023

3.2.6 สิ่งที่ใช้ในการวิจัย

1. Laptop CPU I5, RAM 16 GB, SSD 240GB, Windows 11 64Bit
2. Amazon Elastic Compute Cloud (Amazon EC2) 2 Units (Register-Pay at You Go)
(CentOS 7, Webmin, vCPU 2 Core, Ram 4 GB, HDD 60 GB, 1 Public IP)
3. SIEM Wazuh 4.5 (Open Source), Python3, Notepad++, Putty, WinSCP 6.1
4. VMWare Workstation 16, Kali Linux 2023
5. Slack Service User API (Register-Free)
6. Slack Application on Windows 11 64Bit
7. Internet Speed 10 Mbps

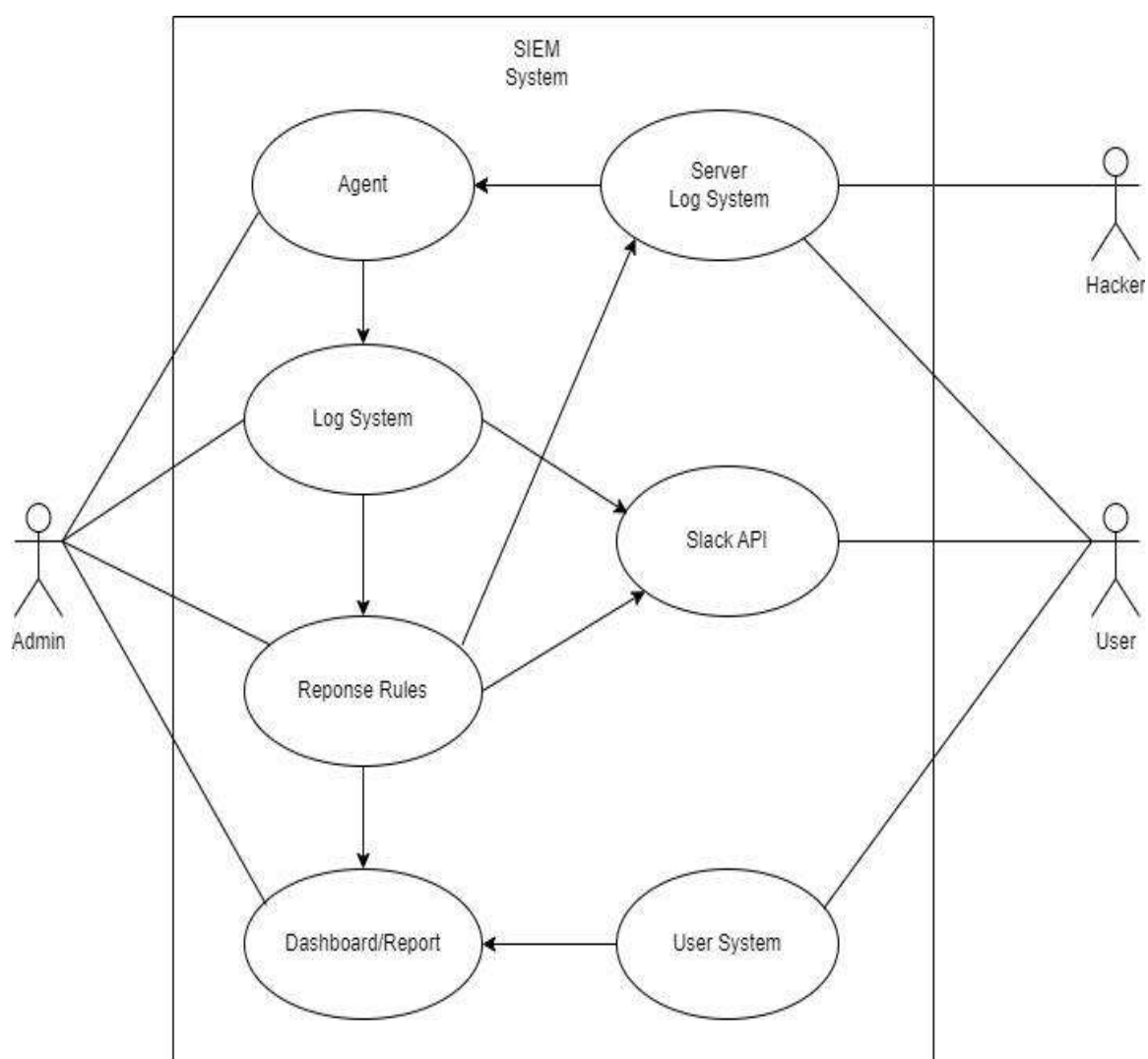
3.3 ออกแบบและพัฒนากการตอบสนองการโจมตีและการแจ้งเตือน

ผู้วิจัยนำข้อมูลที่ได้จากระบบ SIEM มาทำการวิเคราะห์ ออกแบบการตอบสนองการโจมตี โดยศึกษารูปแบบการโจมตีโดยจำลองการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายที่มีการติดตั้ง Agent เรียบร้อยแล้ว จากนั้น ดูเห็นการแจ้งเตือนที่ถูกระบบ SIEM เพื่อนำมาเขียนเงื่อนไขการโจมตี แล้วนำไปตั้งค่าที่อยู่ ค่าติดตั้งระบบ SIEM แล้วตรวจสอบว่าระบบมีการบันทึกตามกำหนดไว้หรือไม่ ดังภาพประกอบที่ 3.22



ภาพประกอบที่ 3.22 แสดง System Design

3.3.1 Use Case Diagram การพัฒนาระบบตามมาตรฐานยูเอ็มแอล เพื่อให้ยูสเคสไดอะแกรมเป็นเทคนิคในการจำลองความต้องการของผู้ใช้งานรวมถึงแสดงความสามารถของระบบ ยูสเคสไดอะแกรมเป็นแผนภาพมาตรฐานที่สามารถอธิบายระบบที่ทำความเข้าใจได้โดยง่าย โดยใช้ในการแสดงฟังก์ชันหลักของระบบซอฟต์แวร์ และเน้นการแสดงความสัมพันธ์ระหว่างผู้ใช้งานและระบบ อีกทั้งแสดงวิธีการทำงานของระบบในแต่ละสถานการณ์ ซึ่งช่วยให้ผู้ออกแบบสามารถสื่อสารกับผู้ใช้งานได้อย่างถูกต้อง และช่วยสร้างความเข้าใจในการทำงานของระบบ รายละเอียดดังภาพประกอบที่ 3.23



ภาพประกอบที่ 3.23 แสดง Use Case Diagram แพลตฟอร์มจัดการ SIEM

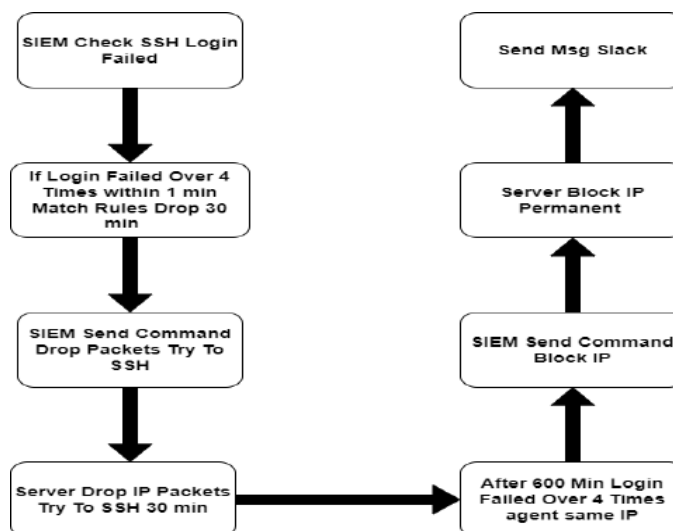
3.3.2 ขั้นตอนการออกแบบเงื่อนไขโดยใช้หลักการบันทึก Log ที่ได้จากการทดสอบในการ พยายาม ไล่ Password จำนวน 5 ครั้งหลังจากนั้นทำการตรวจสอบค่า Log ที่เปรียบเทียบกับค่า MITRE ATT&CK Framework ที่ได้ในตารางมากำหนดค่าใหม่และเขียนเงื่อนไขในไฟล์ Rules ที่กำหนดไว้ใน SIEM เพื่อใช้ ส่งชุดคำสั่งไปให้ Agent สั่งเครื่องคอมพิวเตอร์แม่ข่ายให้ Drop Packets หรือ Block IP รายละเอียด ดัง ภาพประกอบที่ 3.24 และ 3.25

```

GNU nano 2.3.1 File: /var/ossec/etc/rules/local_rules.xml
!-- Local rules -->
<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->
<!-- Example -->
<group name="local,syslog,sshd,">
  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 $
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>
</group>
[ Read 49 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell

```

ภาพประกอบที่ 3.24 แสดงไฟล์กำหนดกฎใน SIEM



ภาพประกอบที่ 3.25 แสดง System Auto Block SSH

เมื่อไฟล์ได้ตามข้อกำหนดกฎไว้เรียบร้อยแล้ว เมื่อเกิดเหตุการณ์ใดที่ SIEM บันทึกแล้วตรงตามกฎ ก็จะทำการส่งการชุดความส่งไปสั่งให้เครื่องคอมพิวเตอร์แม่ข่ายทำตามคำสั่งทันทีเปรียบเทียบข้อกำหนดที่ตั้งไว้ รายละเอียดดังภาพประกอบที่ 3.26

```
<!-- active-response -->
<active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>100020</rules_id>
  <timeout>1800</timeout>
</active-response>
<active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>100030</rules_id>
  <timeout>1800</timeout>
</active-response>
```

ภาพประกอบที่ 3.26 แสดง การตั้งเงื่อนไขการป้องกันแบบเรียลไทม์

เมื่อตรวจการป้องกันเรียบร้อยแล้วระบบ SIEM จะทำการส่งข้อความแจ้งเตือนผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่ายว่ามีความพยายามในการ SSH Brute Force โดยใช้การกำหนดเงื่อนไข เพื่อส่งข้อความผ่านชุดคำสั่งภาษา Python3 ในส่วนชุด Integration ของ SIEM จากรายละเอียดดังภาพประกอบที่ 3.27

```
<integration>
  <name>custom-block</name>
  <hook_url>https://hooks.slack.com/services/T05QKEZ6JQ1/B06CF8C5CR0/91
  <rule_id>100020</rule_id>
  <alert_format>json</alert_format>
</integration>
<integration>
  <name>custom-block</name>
  <hook_url>https://hooks.slack.com/services/T05QKEZ6JQ1/B06CF8C5CR0/91
  <rule_id>100030</rule_id>
  <alert_format>json</alert_format>
</integration>
```

ภาพประกอบที่ 3.27 แสดง การตั้งเงื่อนไขการส่งข้อความทาง Slack

เมื่อระบบตรวจสอบการป้องกันการโจมตีแล้วและอยู่ในเงื่อนไขการส่งข้อความก็จะทำงานตามชุดคำสั่งภาษา Python3 ที่อยู่ในส่วน Integration ตามชื่อไฟล์ที่เรากำหนดไว้ เช่น Slack หรือ Custom-Slack โดย Wazuh จะหาไฟล์ตามที่ชื่อเรากำหนดจากนั้นการรันชุดสั่งโดย Load คำสั่ง Python3 และตามด้วยคำสั่งส่งข้อความทาง API ของ Slack รายละเอียดดังภาพประกอบที่ 3.28 และ 3.29

```
level = alert['rule']['level']

if (level <= 4):
    color = "good"
elif (level >= 5 and level <= 7):
    color = "warning"
else:
    color = "danger"

msg = {}
msg['color'] = color
msg['pretext'] = "Auto Block Alert"
msg['title'] = alert['rule']['description'] if 'description' in alert['rule'] else "N/A"
msg['text'] = alert.get('full_log')

msg['fields'] = []
if 'agent' in alert:
    msg['fields'].append({"title": "Host", "value": "{(0)} - {(1)}".format(alert['agent']['id'], alert['agent']['name']),
    })
msg['fields'].append({"title": "Rule ID", "value": "{0} _ (Level {1}) _".format(alert['rule']['id'], level),
    })

msg['ts'] = alert['id']
attach = {'attachments': [msg]}

return json.dumps(attach)
```

ภาพประกอบที่ 3.28 แสดง การกำหนดพารามิเตอร์ส่งข้อความทาง Slack

ssh: Insecure connection attempt (scan).
 Nov 10 09:04:22 ip-172-31-45-16 sshd[11900]: Did not receive identification string from 220.134.100.75 port 47612
 Host
 (003) - WWW
 Rule ID
 5706 (Level 6)
 Today at 4:04 PM

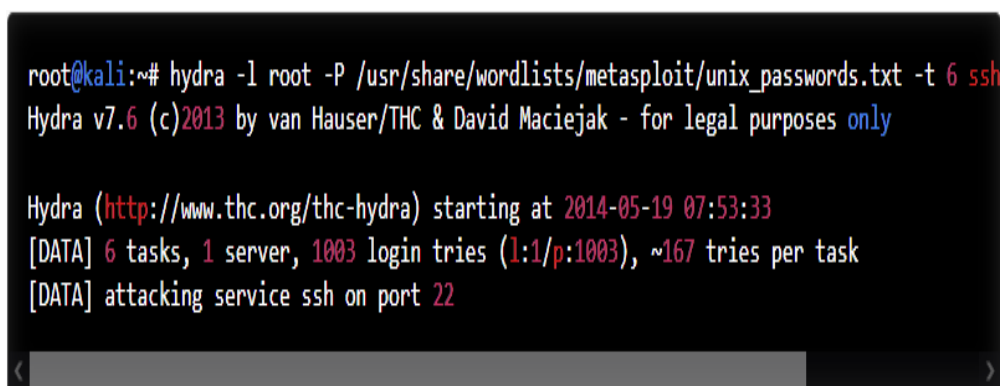
Auto Block Alert
 IP address 101.100.176.99 sshd: Attempt to login using a non-existent user.
 Nov 10 09:05:52 ip-172-31-45-16 sshd[11911]: Invalid user whli2 from 101.100.176.99 port 53902
 Host
 (003) - WWW
 Rule ID
 100040 (Level 10)
 Today at 4:05 PM

ภาพประกอบที่ 3.29 แสดง ข้อความการแจ้งเตือนทาง Slack

3.4 ทดสอบการป้องกันการโจมตีและการแจ้งเตือน

เมื่อผู้วิจัยได้ทำการติดตั้งระบบ SIEM เป็นที่เรียบร้อยแล้ว จึงได้มีการใช้เครื่องมือที่อยู่ใน Kali Linux เป็นเครื่องมือในการทดสอบการโจมตีแบบ SSH Brute Force โดยใช้การทดสอบจำนวน เพื่อใช้ในการสรุปผลการทดสอบ โดยเครื่องมือมีดังต่อไปนี้

3.4.1 Hydra เป็นแครกเกอร์เข้าสู่ระบบแบบขนานซึ่งรองรับโปรโตคอลมากมายในการโจมตี มันรวดเร็วและยืดหยุ่นมาก และสามารถเพิ่มโมดูลใหม่ๆ ได้อย่างง่ายดายเครื่องมือนี้ช่วยให้นักวิจัยและที่ปรึกษาด้านความปลอดภัยสามารถแสดงให้เห็นว่าการเข้าถึงระบบจากระยะไกลโดยไม่ได้รับอนุญาตนั้นง่ายดายเพียงใด ซึ่งรองรับการเข้าถึงแบบ SSH (v1 and v2), SSHKEY ดังภาพประกอบที่ 3.30



```
root@kali:~# hydra -l root -P /usr/share/wordlists/metasploit/unix_passwords.txt -t 6 ssh
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2014-05-19 07:53:33
[DATA] 6 tasks, 1 server, 1003 login tries (1:1/p:1003), ~167 tries per task
[DATA] attacking service ssh on port 22
```

ภาพประกอบที่ 3.30 แสดงเครื่องมือ Hydra

3.4.2 Medusa ได้รับการออกแบบมาให้เป็นหน่วยในการเข้าสู่ระบบที่รวดเร็วและขนานกันอย่างรวดเร็ว เป้าหมายคือการสนับสนุนบริการต่างๆ มากมายที่อนุญาตการตรวจสอบสิทธิ์ระยะไกลให้ได้มากที่สุด เป็นคุณสมบัติหลักบางประการของแอปพลิเคชันนี้ การทดสอบแบบ Brute-force สามารถทำได้กับโฮสต์ ผู้ใช้ หรือรหัสผ่านหลายรายการพร้อมกัน การป้อนข้อมูลของผู้ใช้ที่ยืดหยุ่น ข้อมูลเป้าหมาย (โฮสต์/ผู้ใช้/รหัสผ่าน) ดังภาพประกอบที่ 3.31

```

root@kali:~# medusa -h
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

Syntax: Medusa [-h host|-H file] [-u username|-U file] [-p password|-P file] [-C file] -M
-h [TEXT]      : Target hostname or IP address
-H [FILE]      : File containing target hostnames or IP addresses
-u [TEXT]      : Username to test
-U [FILE]      : File containing usernames to test
-p [TEXT]      : Password to test
-P [FILE]      : File containing passwords to test
-C [FILE]      : File containing combo entries. See README for more information.
-O [FILE]      : File to append log information to
-e [n/s/ns]    : Additional password checks ([n] No Password, [s] Password = Username)
-M [TEXT]      : Name of the module to execute (without the .mod extension)
-m [TEXT]      : Parameter to pass to the module. This can be passed multiple times with
                  different parameter each time and they will all be sent to the module (i
                  -m Param1 -m Param2, etc.)

```

ภาพประกอบที่ 3.31 แสดงเครื่องมือ Medusa

3.4.3 Ncrack เป็นเครื่องมือแคร็กการรับรองความถูกต้องเครือข่ายความเร็วสูง มันถูกสร้างขึ้นเพื่อช่วยการทดสอบโฮสต์ และอุปกรณ์เครือข่ายทั้งหมดเชิงรุกเพื่อหารหัสผ่านที่ไม่ดี ผู้เชี่ยวชาญด้านความปลอดภัยยังพึ่งพา Ncrack เมื่อตรวจสอบลูกค้าของตน Ncrack ได้รับการออกแบบโดยใช้แนวทางแบบโมดูลาร์ ซึ่งเป็นไวยากรณ์บรรทัดคำสั่งที่คล้ายกับ Nmap และเอ็นจินไดนามิกที่สามารถปรับพฤติกรรมตามคำติชมของเครือข่าย ช่วยให้ตรวจสอบโฮสต์จำนวนมากได้อย่างรวดเร็ว และเชื่อถือได้ ซึ่งรองรับการเข้าถึงแบบ RDP, SSH, http(s), SMB, pop3(s), VNC, FTP, and telnet ดังภาพประกอบที่ 3.32

```

root@kali:~# ncrack -h
Ncrack 0.7 ( http://ncrack.org )
Usage: ncrack [Options] {target and service specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iX <inputfilename>: Input from Nmap's -oX XML output format
  -iN <inputfilename>: Input from Nmap's -oN Normal output format
  -iL <inputfilename>: Input from list of hosts/networks
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
SERVICE SPECIFICATION:

```

ภาพประกอบที่ 3.32 แสดงเครื่องมือ Ncrack

3.5 การประเมินประสิทธิภาพการโจมตีแบบเรียลไทม์และแจ้งเตือน

วิเคราะห์ผลข้อมูลความพึงพอใจด้านการทำงานของการป้องกันการโจมตีแบบเรียลไทม์และการแจ้งเตือน มีรูปแบบการวิเคราะห์ทางสถิติ ดังนี้

1. ความพึงพอใจการทำงานระบบป้องกันแบบเรียลไทม์และแจ้งเตือน

การกำหนดระดับค่าคะแนนของแบบสอบถาม ระดับคะแนนของมาตราส่วนประมาณค่า กำหนดระดับค่าคะแนนในการตอบแบบสอบถามเกี่ยวกับความพึงพอใจด้านการทำงานของการป้องกันการโจมตีแบบเรียลไทม์ และความพึงพอใจด้านคุณภาพของระบบ แบ่งออกเป็น 5 ระดับ (Rating Scale) ตามแบบของลิเคิร์ท (Rensis Likert, 1987) รายละเอียดดังตารางที่ 3.1

ตารางที่ 3.1 แสดงระดับ และจำนวนคะแนน

ระดับ	จำนวนคะแนน
มากที่สุด	5
มาก	4
ปานกลาง	3
น้อย	2
น้อยที่สุด	1

เกณฑ์การวัดประมาณค่า (Rating scale) มีทั้งหมด 5 ระดับ และตั้งแต่คะแนนน้อยที่สุดคือ 1 และมากที่สุดคือ 5 โดยการหาค่าคำนวณสามารถใช้สมการ รายละเอียดดังตารางที่ 3.2 (บุญชม ศรีสะอาด, 2545)

$$\begin{aligned}
 \text{อันดับภาคส่วน} &= \frac{\text{คะแนนสูงสุด} - \text{คะแนนต่ำสุด}}{\text{จำนวนชั้น}} \\
 &= \frac{5 - 1}{5} \\
 &= 0.8
 \end{aligned}$$

ตารางที่ 3.2 แสดงระดับค่าเฉลี่ยอันตรภาคชั้น

ค่าเฉลี่ย	ระดับ
4.21 - 5.00	มากที่สุด
3.41 - 4.20	มาก
2.61 - 3.40	ปานกลาง
1.81 - 2.60	น้อย
1.00 - 1.80	น้อยที่สุด

สถิติที่ใช้ในการวิเคราะห์

1. หาค่าเฉลี่ยของคะแนนจากสูตรคำนวณโดยกำหนดค่าคะแนนเป็น 1, 2, 3, 4 และ 5 ตามลำดับ โดยกำหนดระดับการแปรผลโดยใช้สูตรการคำนวณสมการที่ (3.1)

$$\bar{x} = \frac{\sum x}{n} \quad (3.1)$$

แปลค่าคำนวณคะแนนเฉลี่ยเป็น ดังนี้

$$\text{ค่าเฉลี่ยของคะแนน} = \frac{\text{ผลคะแนนรวมทั้งหมด}}{\text{จำนวนข้อรวมทั้งหมด}}$$

2. หาค่าเบี่ยงเบนมาตรฐานการทำงานระบบป้องกันแบบเรียลไทม์ และแจ้งเตือน

การตรวจสอบคุณภาพด้านความเที่ยงตรงของการป้องกันแบบเรียลไทม์ และการแจ้งเตือน เพื่อตรวจสอบคุณภาพ และเพื่อวิเคราะห์หาค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation, SD) คิดค้น โดย เป็นค่าที่ใช้การแสดงความแม่นยำของการทดลองซ้ำๆหลายครั้ง (ค่าความห่างจากค่าเฉลี่ย) ค่าสมการที่ (3.2)

$$S.D. = \sqrt{\frac{\sum (x - \bar{x})^2}{(N-1)}} \quad (3.2)$$

แปลค่าจำนวนเป็นตัวอย่าง ที่รายละเอียดดังตารางที่ 3.3 ไว้ดังนี้

ตารางที่ 3.3 ระดับค่าเบี่ยงเบนมาตรฐานการทดสอบ

ครั้งที่ (N)	X (%)	$(x - \bar{x})$	$(x - \bar{x})^2$
1	90	-3	9.00
2	90	-3	9.00
3	90	-3	9.00
4	95	2	4.00
5	100	7	49.00
Σx	465	$\Sigma(x - \bar{x})^2$	80.00
จำนวนครั้งทดสอบ	N	5	
ค่าเฉลี่ย	$\bar{x}$	93.00	
ค่าเบี่ยงเบน	S.D.	4.47	

การประเมิน และวัดผลลัพธ์เพื่อวิเคราะห์ระดับความแม่นยำในการป้องกันเครื่องคอมพิวเตอร์แม่ข่ายแบบเรียลไทม์ และการแจ้งเตือนที่ได้ออกแบบในงานวิจัย ผู้วิจัยจะใช้เกณฑ์การประเมินประสิทธิภาพการทำงานของระบบจากรูปแบบวิธีการคำนวณความแม่นยำ (Accuracy) เป็นค่าที่บ่งบอกถึงความสามารถของการป้องกันการโจมตี Brute Force เครื่องคอมพิวเตอร์แม่ข่ายด้วยวิธี การป้องกันแบบเรียลไทม์ได้แม่นยำ และสามารถส่งข้อความได้อย่างถูกต้อง

3.6 ข้อจำกัดทางงานวิจัย

การวิจัยเรื่อง การพัฒนาระบบป้องกันภัยคุกคามทางไซเบอร์ของเครื่องคอมพิวเตอร์แม่ข่าย เป็นการศึกษาภายใต้บริบทการพัฒนา ระบบ SIEM ใช้ในการตอบสนองภัยคุกคามที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายโดยอาศัยการวิเคราะห์เงื่อนไข ซึ่งงานวิจัยมีข้อจำกัดของการวิจัยดังนี้

1. ข้อจำกัดของข้อมูล ข้อมูลบันทึกเหตุการณ์จากเครื่องคอมพิวเตอร์แม่ข่ายมีการจัดเก็บที่ระยะเวลาที่จำกัด และความครบถ้วนของจำนวนข้อมูลขณะช่วงการพัฒนา ระบบ ซึ่งบางช่วงเวลาเกิดจากข้อขัดข้องของการปิดเครื่องคอมพิวเตอร์แม่ข่ายได้
2. ข้อจำกัดเรื่องเวลา การวิจัยต้องใช้เวลานานกว่า 7 วันในการเตรียมความพร้อมของระบบเครื่องคอมพิวเตอร์แม่ข่ายเพื่อใช้ในการเป็นแบบล่อเป้าหมาย (Honeypot) และเครื่องคอมพิวเตอร์แม่ข่ายระบบ SIEM เพื่อพร้อมในการเก็บข้อมูลการเข้าถึงเครื่องแม่เพื่อใช้ในการงานวิจัย และวิเคราะห์สรุปผลการวิจัย
3. ข้อจำกัดเรื่องงบประมาณ การวิจัยนี้เป็นงานวิจัยที่ต้องใช้งบประมาณมาก เนื่องจากต้องใช้ระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ในบริการแบบ AWS Cloud Service เพื่อสามารถเก็บข้อมูลจากการโจมตีโดย Honeypot ได้ดี และครบถ้วนกว่าการใช้ระบบปิดจำลองจากเครื่องส่วนตัว
4. ข้อจำกัดของเทคโนโลยี เนื่องจากระบบ SIEM ที่นำมาพัฒนาต่อยอดเป็นแบบ Open Source จึงต้องใช้การวิเคราะห์จาก MITRE ATT&CK อาจมีข้อจำกัดในเรื่องความแม่นยำสูง

3.7 สรุป

1. บทที่ 3 เป็นการนำเสนอวิธีดำเนินการวิจัย ที่ประกอบด้วย ขั้นตอนการดำเนินงานวิจัย เครื่องมือใช้ในการวิจัย ออกแบบและพัฒนา ทดสอบการป้องกันการโจมตี และการแจ้งเตือน การนำไปทดสอบจริง และการประเมินประสิทธิภาพการทำงาน เพื่อใช้ในการตอบคำถามตามวัตถุประสงค์และสมมติฐานที่ได้กำหนดไว้ในบทที่ 1
2. การดำเนินการทางด้านเทคนิคส่วนของ MITRE ATT&CK Framework ที่อยู่ใน SIEM Open Source ที่ไม่มีค่าลิขสิทธิ์ นำมาประยุกต์ใช้งานให้เกิดประโยชน์ในการป้องกันการโจมตีแบบเรียลไทม์ โดยเป็นการลงทุนการรักษาความปลอดภัยทางไซเบอร์ที่มีค่าใช้จ่ายที่คุ้มค่าและต้นทุนต่ำหากเปรียบเทียบกับค่าใช้จ่ายแบบมีค่าลิขสิทธิ์
3. ผลการวิจัยครั้งนี้สามารถนำไปใช้ในการป้องกันภัยทางไซเบอร์แบบเรียลไทม์หากมีการโจมตีผู้มิจฉาชีพหรือชื่อผู้ใช้งาน เช่น การเข้าถึงแบบผู้ดูแล ไม่กำหนดค่าความปลอดภัยที่อยู่ระดับมาตรฐาน ISO 27001

บทที่ 4

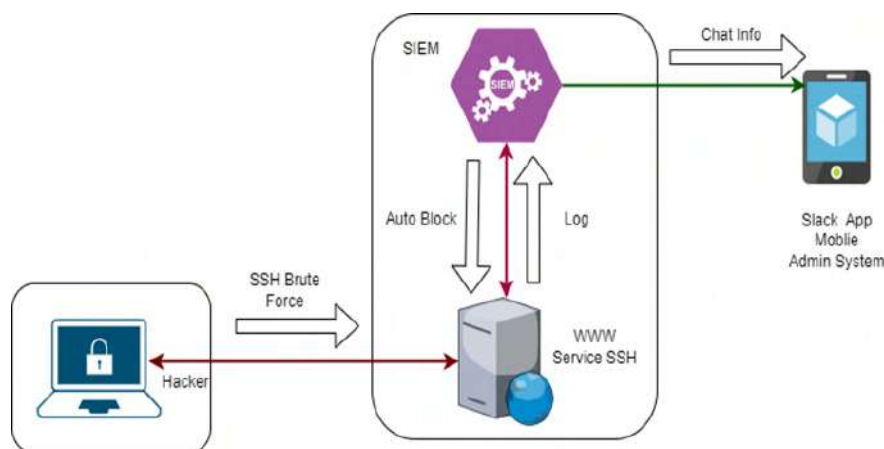
ผลการวิจัย

การศึกษาและวิจัยในครั้งนี้ เป็นการพัฒนาระบบป้องกัน โจมตีแบบเรียลไทม์พร้อมกับการแจ้งเตือน ด้วย Slack Application โดยในการวิจัยมุ่งเน้นในการปรับปรุงและพัฒนาการตอบสนองได้อย่างทันที หากเกิดเหตุการณ์การโจมตีผ่านช่องทาง SSH ซึ่งมักเกิดการโจมตีอย่างต่อเนื่องที่เครื่องคอมพิวเตอร์แม่ข่าย เพื่อป้องกันผู้ที่ไม่หวังดี สามารถเข้าควบคุมเครื่องคอมพิวเตอร์แม่ข่ายได้อย่างสมบูรณ์ และสามารถกระทำการใดๆ ได้แทนผู้ดูแลระบบ โดยการวิจัยมุ่งเน้นประเด็นด้วยกัน 4 หัวข้อ ตามวัตถุประสงค์ที่ได้ตั้งไว้ ดังนี้

1. เพื่อทำการวิเคราะห์ภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายในองค์กร
2. พัฒนาระบบป้องกัน และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์
3. เพื่อทำการประเมินประสิทธิภาพของระบบป้องกัน และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย
4. นำเสนอแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ใหม่ที่เหมาะสมกับองค์กร ภายใต้งานความคิดที่ไม่ไว้วางใจใคร หากแต่ต้องตรวจสอบอยู่เสมอ

ทั้งนี้แนวทางในการวิจัย จะดำเนินการตามแนวทางวงจร System Development Life Cycle (SDLC) จากการทำงานการป้องกันและแจ้งเตือนตามภาพประกอบที่ 4.1 ได้แยกออกเป็น 5 ขั้นตอนได้แก่

1. จัดเตรียมเครื่องมือ และวางแผนการวิจัย
2. เก็บข้อมูลการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายเพื่อออกแบบ และพัฒนาการตอบสนอง
3. ออกแบบพัฒนาการตอบสนองการโจมตี และการแจ้งเตือน
4. ทดสอบระบบป้องกันการโจมตีแบบเรียลไทม์ และการแจ้งเตือน
5. สรุปและประเมินผลการประสิทธิภาพการโจมตีแบบเรียลไทม์ และการแจ้งเตือน



ภาพประกอบที่ 4.1 แสดงขั้นตอนการทำงานของระบบ SIEM

4.1 ผลการวิเคราะห์ภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายในองค์กร

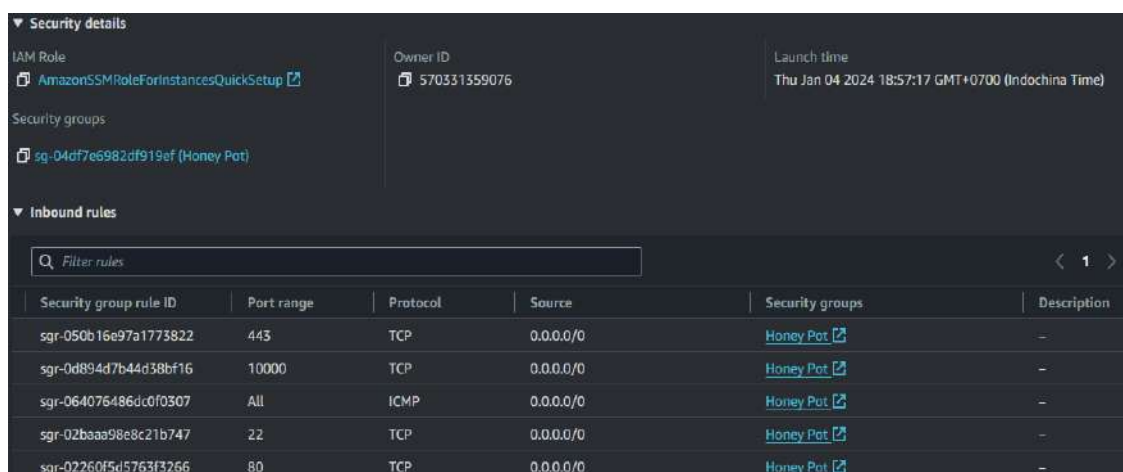
ผลศึกษาวิเคราะห์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่าย คือการมีความเสี่ยงในด้านความมั่นคงปลอดภัยไซเบอร์หรือการคาดการณ์ถึงการทำให้เกิดความเสียหายอันส่งผลกระทบต่อระบบคอมพิวเตอร์ ข้อมูล และอุปกรณ์คอมพิวเตอร์ต่าง ๆ เช่น การโจมตีด้วยไวรัสคอมพิวเตอร์ การบุกรุกเครือข่ายระบบคอมพิวเตอร์โดยที่ไม่ได้รับอนุญาต การขโมยข้อมูลส่วนบุคคล และการปฏิบัติการที่เกี่ยวกับความเป็นอันตรายของระบบเครือข่ายคอมพิวเตอร์

ภัยคุกคามทางไซเบอร์มีความหลากหลายและต้องการการระมัดระวัง และการป้องกันที่เหมาะสมเพื่อป้องกันความเสี่ยงและการเข้าถึงข้อมูลที่ไม่เป็นไปตามกฎหมายหรือไม่ได้รับอนุญาต ภัยคุกคามทางไซเบอร์ที่พบมากที่สุดในปัจจุบันมี 7 ประเภท ดังนี้

- 1) Malware
- 2) Phishing
- 3) SQL Injection Attacks
- 4) Cross-site Scripting (XSS)
- 5) Denial of Service (DoS)
- 6) Man-in-the-Middle Attacks
- 7) Password Attacks

จากผลการศึกษาวิเคราะห์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายในองค์กรทำให้พบว่าการโจมตีแบบ Password Attacks หรือเรียกว่า Simple Brute Force Attacks เป็นการโจมตีที่พบมากที่สุดใน 7 ประเภทที่กล่าวมาข้างต้น ทำให้ผู้วิจัยได้ทำการวิจัยเพื่อทดสอบการติดตาม เฝ้าระวังและแจ้งเตือน และนำไปสู่ผลการพัฒนาการแจ้งเตือนเมื่อเกิดภัยคุกคามแบบ Simple Brute Force Attacks อย่างเรียลไทม์

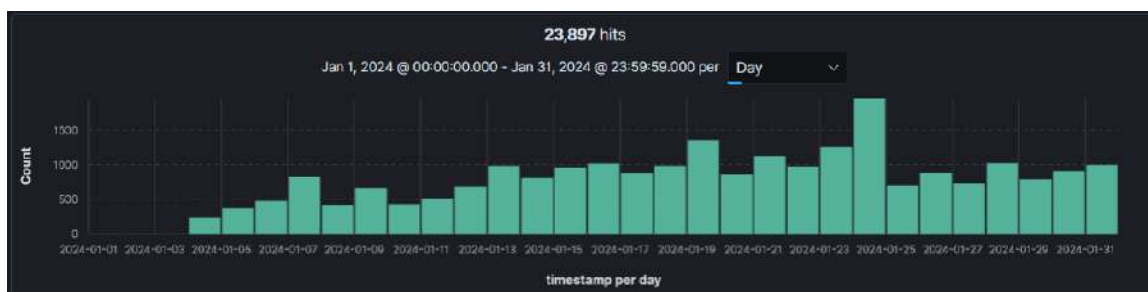
ผู้วิจัยได้ทำการศึกษา และวิเคราะห์ภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายที่เป็นเหยื่อล่อ (Honeypot) และจัดการส่ง Log กิจกรรมที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่าย และทดสอบการแจ้งเตือนไขการป้องกัน พบว่าจากการเก็บข้อมูล และทดสอบผ่านระบบ SIEM ที่ทำการบันทึกกิจกรรมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายผ่านช่อง SSH นั้น เป็นระยะเวลา 1 เดือน ตั้งแต่ วันที่ 1-31 มกราคม 2567 โดยกำหนดการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายเฉพาะ การเข้าแบบ Http, Https, SSH เท่านั้น ดังภาพประกอบที่ 4.2



▼ Security details					
IAM Role		Owner ID		Launch time	
AmazonSSMRoleForInstancesQuickSetup		570331359076		Thu Jan 04 2024 18:57:17 GMT+0700 (Indochina Time)	
Security groups					
sg-04df7e6982df919ef (Honey Pot)					
▼ Inbound rules					
Filter rules					
Security group rule ID	Port range	Protocol	Source	Security groups	Description
sgr-050b16e97a1773822	443	TCP	0.0.0.0/0	Honey Pot	-
sgr-0d894d7b44d38bf16	10000	TCP	0.0.0.0/0	Honey Pot	-
sgr-064076486dc0f0307	All	ICMP	0.0.0.0/0	Honey Pot	-
sgr-02baaa98e8c21b747	22	TCP	0.0.0.0/0	Honey Pot	-
sgr-02260f5d5763f3266	80	TCP	0.0.0.0/0	Honey Pot	-

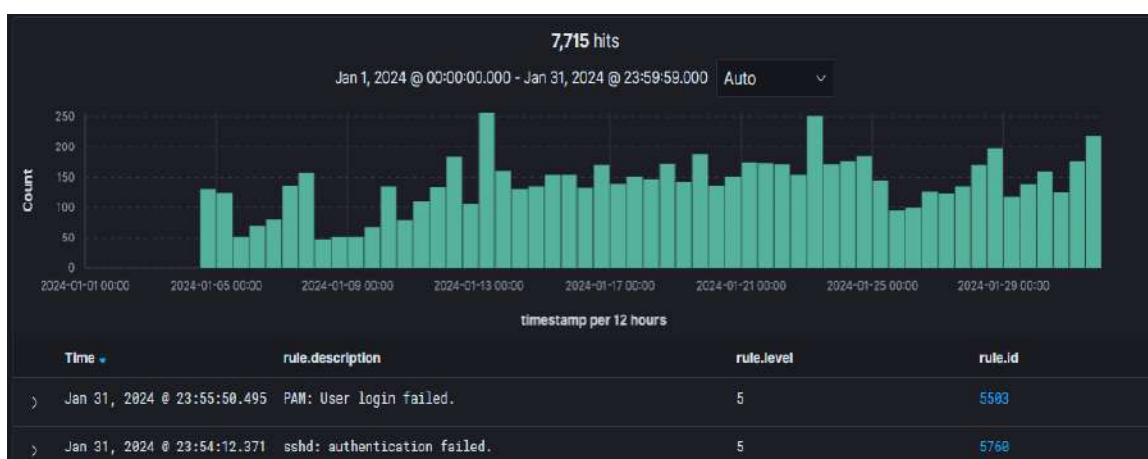
ภาพประกอบที่ 4.2 แสดงการกำหนดเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย Honeypot

ผู้วิจัยพบว่ามีการโจมตีที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายที่เป็น Honeypot ที่ทำการบันทึกจากข้อมูล Log แล้วนำส่งมายังระบบ SIEM เป็นจำนวน 23,897 รายการ ดังภาพประกอบที่ 4.3



ภาพประกอบที่ 4.3 แสดงจำนวนเหตุการณ์บนเครื่องคอมพิวเตอร์แม่ข่าย Honeypot

โดยแยกออกเป็นเหตุการณ์ที่เกิดการโจมตีเครื่องคอมพิวเตอร์แม่ข่าย Honeypot โดยตามสมมุติฐานข้อที่ (1) ภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายในองค์กร มีค่าความร้ายแรงอยู่ในระดับมาก จากการบันทึกพบว่า จำนวน 23,897 รายการ โดยแยกออกเป็นเหตุการณ์ที่เกิดการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายเป็นจำนวน 16,979 รายการ เป็นแบบสุ่มรหัสผ่าน หรือ Brute-Force ทาง port 22 แบบ SSH เป็นจำนวน 15,645 รายการ โดยมีค่าผลการหาค่าเฉลี่ย ($\bar{X}$ = 4.60) อยู่ในระดับมากที่สุด และแยกออกเป็น 2 รูปแบบตาม MITRE ATT&CK TACTICS คือ ชื่อผู้ใช้เป็น Root และไม่ใช่ Root โดยจำนวนผู้ใช้เป็น Root จำนวน 7,715 รายการ และไม่ใช่ Root จำนวน 7,930 รายการ ดังภาพประกอบที่ 4.4 ถึง 4.7



ภาพประกอบที่ 4.4 แสดงจำนวน Rule.id 5503, 5760 สุ่มรหัสผ่านแบบผู้ใช้เป็น Root

```

full_log      Jan 31 12:35:20 ip-172-31-45-16 sshd[20242]: Failed password for root from 42.123.115.126 port 46150 ssh2
id            1706704521.663470
input.type    log
location      /var/log/secure
manager.name  ip-172-31-39-89.ap-southeast-1.compute.internal
predecoder.hostname ip-172-31-45-16
predecoder.program_name sshd
predecoder.timestamp Jan 31 12:35:20
rule.description sshd: authentication failed.
rule.firedtimes 11
rule.gdpr      IV_35.7.d, IV_32.2
rule.gpg13     7.1
rule.groups    syslog, sshd, authentication_failed
rule.hipaa     164.312.b
rule.id        5760

```

ภาพประกอบที่ 4.5 แสดงรายละเอียด Rule.id 5760 สุ่มรหัสผ่านแบบผู้ใช้เป็น Root



ภาพประกอบที่ 4.6 แสดงจำนวน Rule.id 5710 สุ่มรหัสผ่านแบบผู้ใช้ไม่ใช่ Root

```

full_log      Jan 31 16:51:55 ip-172-31-45-16 sshd[1028]: Failed password for invalid user ubnt from 149.23.117.254 port 28577 ssh2
id            1786719916.786399
input.type    log
location      /var/log/secure
manager.name  ip-172-31-35-89.ap-southeast-1.compute.internal
predecoder.hostname ip-172-31-45-16
predecoder.program_name sshd
predecoder.timestamp Jan 31 16:51:55
rule.description sshd: Attempt to login using a non-existent user
rule.firedtimes 8
rule.gdpr      IV.35.7.d, IV.32.2
rule.gpg13     7.1
rule.groups    syslog, sshd, authentication_failed, invalid_login
rule.hipaa     164.312.b
rule.id        5710

```

ภาพประกอบที่ 4.7 แสดงรายละเอียด Rule.id 5710 สุ่มรหัสผ่านแบบไม่ใช่ Root

โดยตรวจสอบพบว่า ผู้โจมตีจะดำเนินการตามขั้นตอนการโจมตี 3 ขั้นตอน ดังนี้

4.1.1 การค้นหาช่องทางบริการเครื่องคอมพิวเตอร์แม่ข่ายที่มีการเปิดการใช้งาน

ผู้โจมตีจะมีการดำเนินการค้นหาเครื่องคอมพิวเตอร์แม่ข่ายที่ทำการเปิด Port การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายที่ทำการเปิดให้สามารถเข้าถึงได้จากภายนอกโดยทำการค้นหาจากเครื่องมือในการค้นหาพอร์ตเพื่อกำหนดการเข้าถึงจากพอร์ตนั้นโดยการทำในขั้นตอนนี้ เป็นส่วนหนึ่งในขั้นตอนการโจมตี โดยกล่าวตาม MITRE ATT&CK TACTICS ขั้นตอนนี้อาจจะมีการทำงานอยู่ 2 ส่วนได้แก่ การลาดตะเวน และการค้นพบ ดังภาพประกอบที่ 4.8 จะแสดงให้เห็นว่าได้มีการเข้ามาค้นหาพอร์ตจำนวน 461 รายการ และรายละเอียดการค้นหาการบริการบนเครื่องคอมพิวเตอร์แม่ข่าย ดังภาพประกอบที่ 4.9



ภาพประกอบที่ 4.8 แสดงการเข้ามาค้นหาพอร์ตเครื่องคอมพิวเตอร์แม่ข่าย

full_log	Jan 31 16:46:31 ip-172-31-45-16 sshd[753]: Did not receive identification string from 223.84.17.16 port 1557
id	1786719591.780295
input.type	log
location	/var/log/secure
manager.name	ip-172-31-39-89.ap-southeast-1.compute.internal
predecoder.hostname	ip-172-31-45-16
predecoder.program_name	sshd
predecoder.timestamp	Jan 31 16:46:31
rule.description	sshd: insecure connection attempt (scan).
rule.firedtimes	1
rule.gdpr	IV_35.7.d
rule.gpg13	4.12
rule.groups	syslog, sshd, recon
rule.id	5706

ภาพประกอบที่ 4.9 แสดงรายละเอียดการค้นหาคำขอการบริการเครื่องคอมพิวเตอร์แม่ข่าย

โดยรายละเอียดการเข้าค้นหาพอร์ตจากผู้โจมตี โดยสามารถแสดงให้เห็นว่าได้มีการเข้าถึงมาจากไอพีต้นทางด้วยหมายเลขอะไร ซึ่งได้แสดงเทคนิคที่ใช้เมื่อเปรียบเทียบกับ MITRE ATT&CK ตามรายละเอียด ดังภาพประกอบที่ 4.10

rule.description	sshd: insecure connection attempt (scan).
rule.firedtimes	1
rule.gdpr	IV_35.7.d
rule.gpg13	4.12
rule.groups	syslog, sshd, recon
rule.id	5706
rule.level	6
rule.mail	false
rule.mitre.id	T1021.004
rule.mitre.tactic	Lateral Movement
rule.mitre.technique	SSH

ภาพประกอบที่ 4.10 แสดงเทคนิคเปรียบเทียบกับ MITRE ATT&CK

4.1.2 การโจมตีเครื่องคอมพิวเตอร์แม่ข่ายแบบสุ่มรหัสผ่าน หรือ Brute Force

ผู้โจมตีเครื่องคอมพิวเตอร์แม่ข่าย เมื่อได้ทราบถึงการบริการเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการอยู่จะพบว่า มีการใช้งาน SSH จากนั้น มีความพยายามเข้าโจมตีเครื่องคอมพิวเตอร์แม่ข่ายด้วยการสุ่มรหัสผ่าน หรือ Brute Force ผ่านช่องทาง SSH เพื่อพยายามเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย เมื่อเปรียบเทียบกับเงื่อนไขของ MITRE ATT&CK จะพบว่ามีแบบสุ่มชื่อผู้ใช้งาน และรหัสผู้ใช้งาน ในแบบต่าง ๆ เพื่อให้สามารถเข้ายึดครองเครื่องคอมพิวเตอร์แม่ข่ายได้ ดังภาพประกอบที่ 4.5 และ 4.7 จากรายละเอียดตามการแยกของเงื่อนไขแบบการสุ่มรหัสผ่านที่แสดงในข้างต้น จะพบว่าระบบ SIEM ได้มีการกำหนด rule.id และ rule.mitre.id ตามภาพประกอบที่ 4.11 ที่สามารถนำไปใช้ในการเขียนเงื่อนไขในไฟล์ XML ของระบบ SIME เพื่อกำหนดเงื่อนไขใหม่

rule.description	sshd: Attempt to login using a non-existent user
rule.firedtimes	8
rule.gdpr	IV_35.7.d, IV_32.2
rule.gpg13	7.1
rule.groups	syslog, sshd, authentication_failed, invalid_login
rule.hipaa	164.312.b
rule.id	5710
rule.level	5
rule.mail	false
rule.mitre.id	T1110.001, T1021.004
rule.mitre.tactic	Credential Access, Lateral Movement
rule.mitre.technique	Password Guessing, SSH

ภาพประกอบที่ 4.11 แสดงรายละเอียด rule.id และ rule.mitre.id

4.1.3 การเข้าเครื่องคอมพิวเตอร์แม่ข่ายอย่างสมบูรณ์

ขั้นตอนนี้เป็นแสดงให้เห็นว่าหากมีการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายได้แบบสมบูรณ์ ระบบ SIEM ก็ยังสามารถระบุการเข้าถึงอย่างสมบูรณ์ในรูปแบบเงื่อนไข rule.id ได้เช่นกัน ซึ่งจากการ

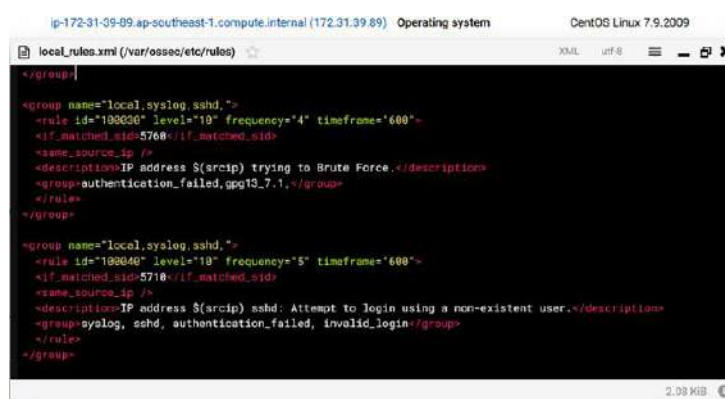
ทดสอบของผู้วิจัยจะพบเป็นการเข้าถึงจากเครื่องต้นทางของผู้วิจัยเองจำนวน 3 รายการ ดังภาพประกอบที่ 4.12



ภาพประกอบที่ 4.12 แสดงรายละเอียดเข้าเครื่องคอมพิวเตอร์แม่ข่ายอย่างสมบูรณ์

4.2 ผลการพัฒนาระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์

จากการรวบรวมข้อมูลจากหัวข้อ 4.1 ผู้วิจัยได้นำมาพัฒนาระบบป้องกันและการแจ้งเตือนภัยคุกคามทางไซเบอร์ โดยนำค่า rule.id และ rule.mitre.id ดังภาพประกอบที่ 4.13



ภาพประกอบที่ 4.13 แสดงรายละเอียดเงื่อนไขพฤติกรรมการโจมตีเครื่องคอมพิวเตอร์แม่ข่าย

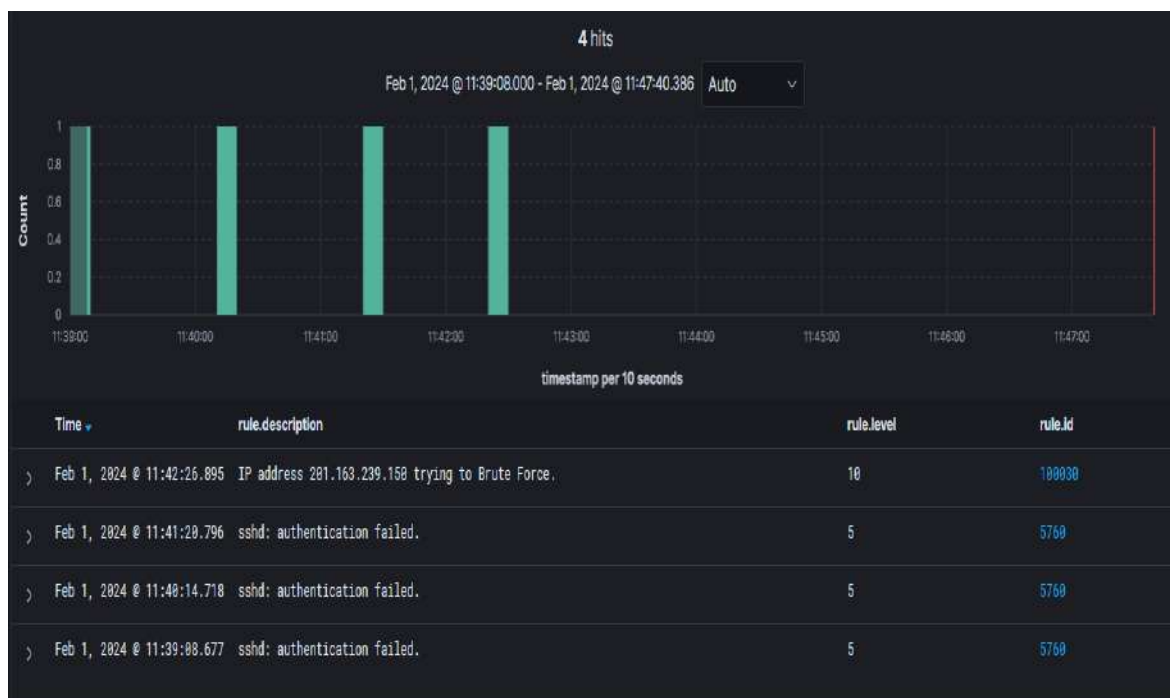
มากำหนดเงื่อนไขในค่าพารามิเตอร์ของ XML ไฟล์ที่เป็นข้อกำหนดของกฎที่ใช้ระบุภัยคุกคามที่เกิดขึ้นจากการ Brute Force SSH ซึ่งค่าพารามิเตอร์ นั้นผู้วิจัยพบว่าสามารถกำหนดด้วย rule.id จำนวน

ครั้ง ขอบเขตระยะเวลาที่กำหนด และไอพีต้นทางเดียวกัน ของเหตุการณ์นั้นๆ เพื่อใช้ประเมิน พฤติกรรมการโจมตีเครื่องคอมพิวเตอร์แม่ข่าย แล้วนำมากำหนด เป็นเงื่อนไข

จากรายละเอียดที่แสดง ดังภาพประกอบที่ 4.13 ได้มีการกำหนดเงื่อนไขการตอบสนองออกเป็น 2 เงื่อนไข รายละเอียดดังนี้

1. เงื่อนไข rule.id = 100030 มีการกำหนดให้หากมีการ สุ่มรหัสผ่านแบบใช้ชื่อ Root ที่เป็น rule.id = 5760 เกิดจากไอพีเดียวกันและเกิดเหตุซ้ำ 4 ครั้งภายในระยะ 10 นาที ให้ตกเงื่อนไขนี้
2. เงื่อนไข rule.id = 100040 มีการกำหนดให้หากมีการ สุ่มรหัสผ่านแบบไม่ใช่ Root ที่เป็น rule.id = 5710 เกิดจากไอพีเดียวกันและเกิดเหตุซ้ำ 5 ครั้งภายในระยะ 10 นาที ให้ตกเงื่อนไขนี้

เมื่อทำการกำหนดเงื่อนไขแล้ว จึงทำการนำทดสอบเพื่อตรวจสอบการทำงานของเงื่อนไขที่กำหนด ปรากฏว่าสามารถใช้เวลาตั้งแต่เริ่มต้น จนเสร็จสิ้นการทำงานไม่เกิน 5 วินาที ซึ่งเป็นการตอบสนอง ใกล้เคียงเวลาเรียลไทม์และยังสามารถเพื่อใช้ในการป้องกันและแจ้งเตือนได้ ดังภาพประกอบที่ 4.14



ภาพประกอบที่ 4.14 แสดงทดสอบเงื่อนไข rule.id = 100030



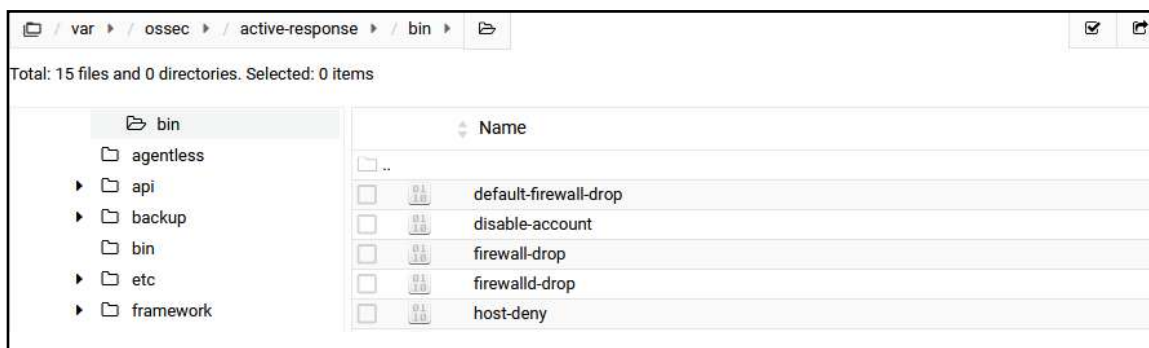
ภาพประกอบที่ 4.15 แสดงทดสอบเงื่อนไข rule.id = 100040

ผลการทดสอบเงื่อนไขที่ได้กำหนดขึ้นมาใหม่จาก rule.id คือ 5760 และ 5710 สามารถทำงานได้ตรงตามเงื่อนไขกำหนด และสามารถแสดงค่าเงื่อนไขใหม่ ในการบันทึก Log ในระบบ SIEM ได้อย่างถูกต้อง จากนั้นจึงนำค่าเงื่อนไขทั้งสอง มาใช้ในการแจ้งเตือน โดยนำค่าเงื่อนไขที่ได้ไปกำหนดค่าพารามิเตอร์ในส่วนการตั้งค่าการตอบสนอง หรือ Active Response เพื่อให้ส่งชุดคำสั่งไปยังเครื่องแม่ผ่าน Agent ที่ได้ติดตั้งไว้ในเครื่องคอมพิวเตอร์แม่ข่ายเพื่อการระงับการเข้าถึง หรือ Block การเข้าถึงจากไอพีต้นทางที่ได้ทำการ Brute Force SSH ที่เข้าเงื่อนไข rule.id คือ 100030 และ 100040 จากภาพประกอบที่ 4.16

```
<!-- active-response -->
<active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>100020</rules_id>
  <timeout>1800</timeout>
</active-response>
<active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>100030</rules_id>
  <timeout>1800</timeout>
</active-response>
<active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>100040</rules_id>
  <timeout>1800</timeout>
</active-response>
<!-- Log analysis -->
```

ภาพประกอบที่ 4.16 แสดงเงื่อนไขส่งชุดคำสั่งไปเครื่องคอมพิวเตอร์แม่ข่ายสำหรับระงับการเข้าถึง

เมื่อการ Brute Force SSH ที่เข้าเงื่อนไข rule id คือ 100030 และ 100040 ก็จะส่งคำสั่งไปยังส่วนที่อยู่ใน Active Response และจะส่งชื่อชุดคำสั่งตามที่เรากำหนดคือ firewall-drop หมายถึงให้ Firewall ที่อยู่ในระบบปฏิบัติการ CentOS7 ทำการ Drop Packet ที่มาจากไอพีต้นทางที่มาจากเงื่อนไข 100030 และ 100040 เพื่อเป็นการระงับการพยายาม Brute Force SSH ในครั้งถัดไป ดังภาพประกอบที่ 4.17



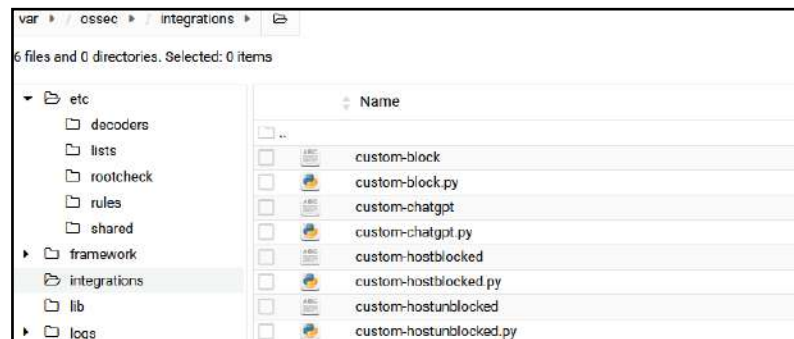
ภาพประกอบที่ 4.17 แสดงเงื่อนไขส่งชุดคำสั่งการป้องกันไปยังเครื่องคอมพิวเตอร์แม่ข่ายผ่าน Agent

จาก rule.id คือ 5760 และ 5710 สามารถทำงานได้ตรงตามเงื่อนไขกำหนด ได้นำค่าเงื่อนไขนี้ไปตั้งกำหนดในการแจ้งเตือนไปยังผู้ดูแลระบบให้ทราบถึงภัยคุกคามไปที่ Application Slack โดยการกำหนดค่าเงื่อนไขใน ค่าติดตั้งของระบบ SIEM ในส่วนของ Interface เพื่อระบบการส่งข้อความและรายละเอียดที่ได้กำหนดให้ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่าย ทราบชนิดภัยคุกคามที่เกิดขึ้นสถานะการณ์การป้องกันเป็นอย่างไร ซึ่งหากเข้าเงื่อนไข rule.id คือ 100030 และ 100040 จากภาพประกอบที่ 4.18

```
<integration>
  <name>custom-block</name>
  <hook_url>https://hooks.slack.com/services/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</hook_url>
  <rule_id>100030</rule_id>
  <alert_format>json</alert_format>
</integration>
<integration>
  <name>custom-block</name>
  <hook_url>https://hooks.slack.com/services/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</hook_url>
  <rule_id>100040</rule_id>
  <alert_format>json</alert_format>
</integration>
```

ภาพประกอบที่ 4.18 แสดงเงื่อนไขส่งชุดคำสั่งการแจ้งเตือนไปยัง Slack ผ่าน API

เมื่อระบบ SIEM ตรวจพบว่าเหตุการณ์ที่เกิดขึ้นตรงตามเงื่อนไขที่กำหนดไว้ใช้ชุดคำสั่งไฟล์การตั้งค่า Integration ของไฟล์ config ของระบบ SIEM ก็จะทำการเรียกชุดคำสั่งไพทอน ที่อยู่ส่วนชุดคำสั่ง Integrations ดังภาพประกอบที่ 4.19



ภาพประกอบที่ 4.19 แสดงเงื่อนไขส่งชุดคำสั่งการแจ้งเตือนไปยัง Slack ผ่าน API

เพื่อเรียกชุดคำสั่ง custom-block ที่ผู้วิจัยได้ทำการเขียนด้วยภาษาไพทอน ดังภาพประกอบที่ 4.20 ใช้ในการอ่านค่า Log ที่บันทึกไว้ในระบบ SIEM เพื่อส่งรายละเอียดไปยัง Slack เพื่อแสดงรายละเอียดให้ผู้ดูแลระบบทราบถึงภัยคุกคามที่เกิดขึ้น ตามเงื่อนไขที่กำหนดในพารามิเตอร์ชุดคำสั่งไพทอนที่ผู้วิจัยได้ระบุไว้แล้ว

```
def generate_msg(alert):
    level = alert['rule']['level']

    if (level <= 4):
        color = "good"
    elif (level >= 5 and level <= 7):
        color = "warning"
    else:
        color = "danger"

    msg = {}
    msg['color'] = color
    msg['pretext'] = "Auto Block Alert"
    msg['title'] = alert['rule']['description'] if 'description' in alert['rule'] else "N/A"
    msg['text'] = alert.get('full_log')

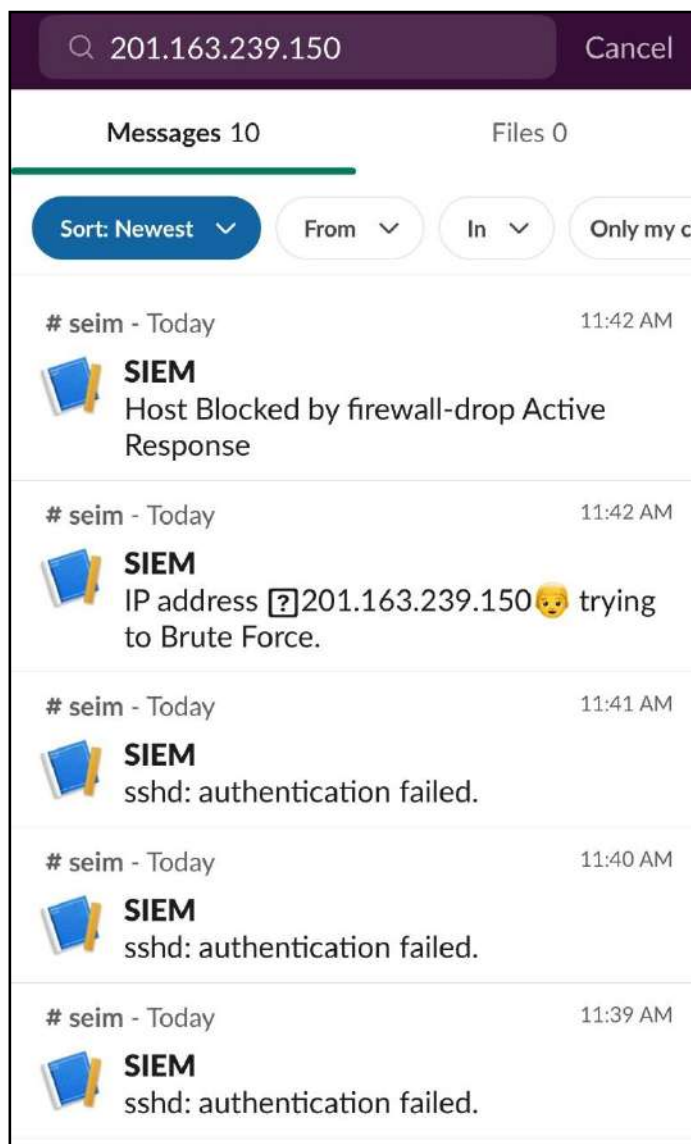
    msg['fields'] = []
    if 'agent' in alert:
        msg['fields'].append({'title': 'Host', 'value': "{0} - {1}".format(alert['agent']['id'], alert['agent']['name'])})
    msg['fields'].append({'title': 'Rule ID', 'value': "{0} _{1}_".format(alert['rule']['id'], level)})

    msg['ts'] = alert['id']
    attach = {'attachments': [msg]}

    return json.dumps(attach)
```

ภาพประกอบที่ 4.20 แสดงเงื่อนไขภาษาไพทอนเป็นรูปแบบ Json ไปยัง Slack ผ่าน API

จากภาพประกอบที่ 4.21 จะเห็นว่าการแจ้งเตือนจะเป็นช่วงขณะเดียวกันกับการป้องกันการโจมตีระบบ SIEM สามารถที่ป้องกันและแจ้งเตือนภัยคุกคาม เครื่องคอมพิวเตอร์แม่ข่ายที่ถูกโจมตี Brute Force SSH ในเวลาเดียวกัน ซึ่งเป็นรวดเร็วขึ้นตอนการประมวลผลของระบบ SIEM และลดขั้นตอนทำให้ระยะเวลาการตอบสนองได้ใกล้เคียงเวลาริยลโหม่มากที่สุด จากกระบวนการครบตามเงื่อนไขสามารถใช้เวลาไม่เกิน 3 วินาที ตามภาพประกอบที่ 4.22 และ 4.23



ภาพประกอบที่ 4.21 แสดงข้อความการแจ้งเตือน Slack ผ่าน Application

full_log	Feb 1 11:42:25 ip-172-31-45-16 sshd[4959]: Failed password for root from 201.163.239.150 port 23695 ssh2
id	1706762546.268668
input.type	log
location	/var/log/secure
manager.name	ip-172-31-39-89.ap-southeast-1.compute.internal
predecoder.hostname	ip-172-31-45-16
predecoder.program_name	sshd
predecoder.timestamp	Feb 1 11:42:25
previous_output	Feb 1 11:41:20 ip-172-31-45-16 sshd[4949]: Failed password for root from 201.163.239.150 port 29789 ssh2 Feb 1 11:40:14 ip-172-31-45-16 sshd[4947]: Failed password for root from 201.163.239.150 port 3183 ssh2 Feb 1 11:39:07 ip-172-31-45-16 sshd[4908]: Failed password for root from 201.163.239.150 port 32205 ssh2
rule.description	IP address 201.163.239.150 trying to Brute Force.
rule.firedtimes	4
rule.frequency	4

ภาพประกอบที่ 4.22 แสดงค่าการโจมตีตรงเงื่อนไขการป้องกัน Brute Force SSH

data.parameters.alert.predecoder.timestamp	Feb 1 11:42:25
data.parameters.alert.previous_output	Feb 1 11:41:20 ip-172-31-45-16 sshd[4949]: Failed password for root from 201.163.239.150 port 29789 ssh2 Feb 1 11:40:14 ip-172-31-45-16 sshd[4947]: Failed password for root from 201.163.239.150 port 3183 ssh2 Feb 1 11:39:07 ip-172-31-45-16 sshd[4908]: Failed password for root from 201.163.239.150 port 32205 ssh2
data.parameters.alert.rule.description	IP address 201.163.239.150 trying to Brute Force.
data.parameters.alert.rule.firedtimes	4
data.parameters.alert.rule.frequency	4
data.parameters.alert.rule.gpg13	7.1
data.parameters.alert.rule.groups	local, syslog, sshd, authentication_failed
data.parameters.alert.rule.id	100030
data.parameters.alert.rule.level	10
data.parameters.alert.rule.mail	false
data.parameters.alert.timestamp	2024-02-01T11:42:26.895+0700
data.parameters.extra_args	
data.parameters.program	active-response/bin/firewall-drop
data.srcip	201.163.239.150

ภาพประกอบที่ 4.23 แสดงการป้องกัน Brute Force SSH แบบเรียลไทม์

4.3 ผลการประเมินประสิทธิภาพของระบบป้องกัน และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย

เมื่อการวิจัยด้านการวิเคราะห์ การป้องกัน และการแจ้งเตือนจากภัยคุกคามทางไซเบอร์เครื่องคอมพิวเตอร์แม่ข่ายแบบเรียลไทม์ ซึ่งประเมินการทำงานของระบบ SIEM จากทดสอบประสิทธิภาพของการวิเคราะห์การป้องกัน และการแจ้งเตือนภัยคุกคาม แบบเรียลไทม์ที่เกิดกับ Honeypot

4.3.1 การประเมินประสิทธิภาพที่มีต่อการทำงานของระบบติดตาม เฝ้าระวัง และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองแบบเรียลไทม์ มีลักษณะเป็นแบบมาตราส่วนประมาณค่า 5 ระดับ (Rating Scale) แบบลิเคิร์ต (Likert)

ซึ่งเกณฑ์การวัดประมาณค่า (Rating scale) มีทั้งหมด 5 ระดับ และตั้งแต่คะแนนน้อยที่สุดคือ 1 และมากที่สุดคือ 5 รายละเอียดดังสมการที่ (4.1)

$$\text{อันตรภาคชั้น} = \frac{\text{คะแนนสูงสุด} - \text{คะแนนต่ำสุด}}{\text{จำนวนชั้น}} \quad (4.1)$$

ค่าเฉลี่ย 4.21 – 5.00 หมายถึง มีประสิทธิภาพในระดับมากที่สุด

ค่าเฉลี่ย 3.41 – 4.20 หมายถึง มีประสิทธิภาพในระดับมาก

ค่าเฉลี่ย 2.61 – 3.40 หมายถึง มีประสิทธิภาพในระดับปานกลาง

ค่าเฉลี่ย 1.81 – 2.60 หมายถึง มีประสิทธิภาพในระดับน้อย

ค่าเฉลี่ย 1.00 – 1.80 หมายถึง มีประสิทธิภาพในระดับน้อยที่สุด

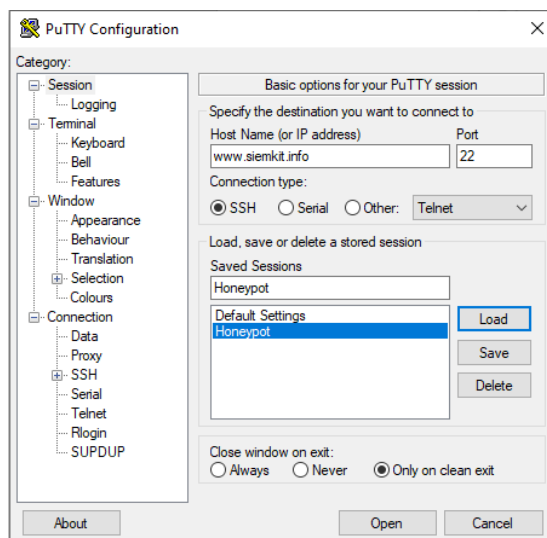
การตรวจสอบคุณภาพด้านความเที่ยงตรงของการติดตาม เฝ้าระวังและการแจ้งเตือนแบบเรียลไทม์เพื่อตรวจสอบคุณภาพและเพื่อวิเคราะห์หาค่าเฉลี่ย ($\bar{X}$) จากสมการหาค่าเฉลี่ยการทดสอบทั้งหมดจำนวน 5 ครั้ง รายละเอียดดังสมการที่ (4.2)

$$\text{ค่าเฉลี่ย} = \frac{\text{ผลรวมค่าระดับทั้งหมด}}{\text{จำนวนครั้งที่ทำการทดสอบ}} \quad (4.2)$$

จากกำหนดประสิทธิภาพ การวิเคราะห์ แจ้งเตือน และป้องกันภัยคุกคามทางไซเบอร์เครื่องคอมพิวเตอร์แม่ข่าย แบบ Brute Force SSH ซึ่งกำหนดไว้ว่า ทำงานครบเงื่อนไขไม่เกิน 5 วินาที จะอยู่ในระดับ 5 ซึ่งจากการทำงานของระบบ SIEM สามารถเก็บค่าการโจมตีที่ได้จากเครื่องคอมพิวเตอร์แม่ข่ายที่ทำการเป็นเหยื่อและทำการวิเคราะห์จากข้อมูลที่แสดงการจำลองการโจมตี Brute Force Attack เครื่องคอมพิวเตอร์แม่ข่ายจำนวน 4 ครั้งต่อ 1 ชุด การโจมตี โดยค่าที่ได้ จากการทดสอบจำนวน 5 ชุด เพื่อคำนวณค่าเฉลี่ย ($\bar{X}$) ว่าอยู่ในระดับใด จากระยะเวลาป้องกันและแจ้งเตือน โดยเปรียบเทียบเวลาตอบสนองจาก Firewall ที่ใช้ในองค์กรทั่วไป ที่ถูกบันทึกในระบบ SIEM ตามภาคผนวก ก ซึ่งมีรายละเอียดดังนี้

ระยะเวลาป้องกันและแจ้งเตือน	1 วินาที – 5 วินาที หมายถึงอยู่ในระดับ 5
ระยะเวลาป้องกันและแจ้งเตือน	6 วินาที – 10 วินาที หมายถึงอยู่ในระดับ 4
ระยะเวลาป้องกันและแจ้งเตือน	11 วินาที – 15 วินาที หมายถึงอยู่ในระดับ 3
ระยะเวลาป้องกันและแจ้งเตือน	16 วินาที – 20 วินาที หมายถึงอยู่ในระดับ 2
ระยะเวลาป้องกันและแจ้งเตือน	25 วินาที – 30 วินาที หมายถึงอยู่ในระดับ 1

ผู้วิจัยได้ทำการทดสอบตามเงื่อนไขที่กำหนด โดยการเชื่อมต่อเข้าเครื่องคอมพิวเตอร์แม่ข่ายที่เป็น Honeypot ด้วยโปรแกรม Putty SSH ทาง Port 22 ดังภาพประกอบที่ 4.24 เพื่อจำลองภัยคุกคามที่ความพยายามเข้าเครื่องคอมพิวเตอร์แม่ข่ายแบบ Brute Force SSH ผลการทดสอบที่ตาราง 4.1 ถึง 4.4



ภาพประกอบที่ 4.24 แสดงเครื่องมือที่ใช้ในการทดสอบ Brute Force SSH

ตารางที่ 4.1 ผลระยะเวลาการป้องกันแบบเรียลไทม์ เงื่อนไขที่ 100030

วัน	1-Feb-24	1-Feb-24	1-Feb-24	1-Feb-24	1-Feb-24	รวม	N	$\bar{x}$
เวลา	13.46.59	13.52.25	14.35.37	14.51.18	15.40.04			
ครั้งที่	1	2	3	4	5	25	5	5.00
ระดับ	5	5	5	5	5			

ตารางที่ 4.2 ผลระยะเวลาการป้องกันแบบเรียลไทม์ เงื่อนไขที่ 100040

วัน	1-Feb-24	1-Feb-24	1-Feb-24	1-Feb-24	1-Feb-24	รวม	N	$\bar{x}$
เวลา	16.04.46	16.22.24	16.35.16	16.49.26	17.01.31			
ครั้งที่	1	2	3	4	5	25	5	5.00
ระดับ	5	5	5	5	5			

ตารางที่ 4.3 ผลระยะเวลาการแจ้งเตือนแบบเรียลไทม์ เงื่อนไขที่ 100030

วัน	1-Feb-24	1-Feb-24	1-Feb-24	1-Feb-24	1-Feb-24	รวม	N	$\bar{x}$
เวลา	13.46.59	13.52.25	14.35.37	14.51.18	15.40.04			
ครั้งที่	1	2	3	4	5	25	5	5.00
ระดับ	5	5	5	5	5			

ตารางที่ 4.4 ผลระยะเวลาการแจ้งเตือนแบบเรียลไทม์ เงื่อนไขที่ 100040

วัน	1-Feb-24	1-Feb-24	1-Feb-24	1-Feb-24	1-Feb-24	รวม	N	$\bar{x}$
เวลา	16.04.46	16.22.24	16.35.16	16.49.26	17.01.31			
ครั้งที่	1	2	3	4	5	25	5	5.00
ระดับ	5	5	5	5	5			

จากการประเมินประสิทธิภาพของระบบป้องกัน และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย แบบเรียลไทม์ ตามสมมุติฐานข้อที่ (2) ระบบป้องกัน และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ มีประสิทธิภาพอยู่ในระดับมาก จะพบว่าผลการทดสอบจากค่าบันทึกในตารางที่ 4.1 ถึง 4.4 ได้แสดงค่าผลการหาค่าเฉลี่ย ($\bar{X}$ = 5.00) อยู่ในระดับ มากที่สุด

4.3.2 การประเมินระบบป้องกัน และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย โดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ มีความเหมาะสม และยอมรับอยู่ในระดับมาก ผู้วิจัยนำแบบประเมินให้กลุ่มเป้าหมายทำการประเมินความเหมาะสมและการยอมรับโดยใช้แบบสอบถามประมาณค่า 5 ระดับ

ในหัวข้อนี้เป็นการประเมินความพึงพอใจผู้ใช้แอปพลิเคชันแบ่งออกเป็น 3 ส่วน คือ

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบประเมิน

ส่วนที่ 2 ความพึงพอใจต่อการใช้งานแอปพลิเคชันสำหรับป้องกันและแจ้งเตือนภัย

คุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายที่มีความทนทานและความ
แม่นยำสูง

ส่วนที่ 3 ข้อเสนอแนะ

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบประเมิน

การสอบถามในครั้งนี้เป็นผู้ใช้ระบบ SIEMKIT ในประเทศไทยจำนวน 68 ท่านมีดังต่อไปนี้
จากรายละเอียดตามตารางที่ 4.5 ถึง 4.10 ดังนี้

ตารางที่ 4.5 ข้อมูลเพศของผู้ตอบแบบประเมิน

เพศ	จำนวน	ค่าเฉลี่ย
ชาย	38	56%
หญิง	30	44%
รวม	68	100%

ตารางที่ 4.6 ข้อมูลอายุของผู้ตอบแบบประเมิน

อายุ	จำนวน	ค่าเฉลี่ย
ต่ำกว่า 30 ปี	19	28%
30-40 ปี	31	46%
41-50 ปี	13	19%
51-60 ปี	5	7%
60 ปีขึ้นไป	0	0%
รวม	68	100%

ตารางที่ 4.7 ข้อมูลระดับการศึกษาของผู้ตอบแบบประเมิน

ระดับการศึกษา	จำนวน	ค่าเฉลี่ย
ต่ำกว่าปริญญาตรี	2	3%
ปริญญาตรี	46	68%
ปริญญาโท	17	25%
ปริญญาเอก	3	4%
รวม	68	100%

ตารางที่ 4.8 ข้อมูลประสบการณ์ทำงานของผู้ตอบแบบประเมิน

ประสบการณ์ทำงาน	จำนวน	ค่าเฉลี่ย
น้อยกว่า 3 ปี	12	18%
3-5 ปี	20	29%
6-10 ปี	12	18%
มากกว่า 10 ปี	24	35%
รวม	68	100%

ตารางที่ 4.9 ข้อมูลของประเภทหน่วยงาน

ระดับการศึกษา	จำนวน	ค่าเฉลี่ย
ภาครัฐ	4	6%
ภาคเอกชน	60	88%
ภาครัฐวิสาหกิจ	2	3%
อื่นๆ	2	3%
รวม	68	100%

ตารางที่ 4.10 ข้อมูลการดำเนินงานของหน่วยงาน

ระดับการศึกษา	จำนวน	ค่าเฉลี่ย
บริการ	44	65%
ผลิตภัณฑ์	11	16%
การค้า	4	6%
อื่นๆ	9	13%
รวม	68	100%

ส่วนที่ 2 ระดับความพึงพอใจต่อการใช้งานแอปพลิเคชันสำหรับป้องกันและแจ้งเตือน

ภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายฯ

ขอความกรุณาท่านได้โปรดพิจารณาข้อคำถามดังต่อไปนี้ แล้วทำเครื่องหมาย ☒ ลงในช่องที่ตรงกับความจริง ความคิดเห็น หรือความรู้สึกของท่านมากที่สุดเพียงช่องเดียว ทั้งนี้ผู้วิจัยได้แบ่งระดับคำตอบไว้เป็น 5 ระดับ จากรายละเอียดตามตารางที่ 4.11 ถึง 4.15 ดังนี้

5 หมายถึง ระดับพึงพอใจมากที่สุด

4 หมายถึง ระดับพึงพอใจมาก

3 หมายถึง ระดับพึงพอใจปานกลาง

2 หมายถึง ระดับพึงพอใจน้อย

1 หมายถึง ระดับพึงพอใจน้อยที่สุด

ตารางที่ 4.11 ผลการประเมินด้านระบบตรงกับความต้องการของผู้ใช้

ข้อที่	ข้อความถาม	ผลการประเมิน		
		$\bar{X}$	S.D.	แปลผล
1	ความสามารถของระบบในการจัดการแจ้งเตือนการโจมตีทางไซเบอร์ได้อย่างรวดเร็ว	4.21	0.86	มากที่สุด
2	ความสามารถของระบบในการจัดการป้องกันการโจมตีทางไซเบอร์ได้อย่างรวดเร็ว	4.07	0.80	มาก
3	ความสามารถของระบบในการแสดงข้อมูลได้อย่างรวดเร็ว	4.26	0.78	มากที่สุด
4	ความสามารถของระบบในการค้นหาข้อมูลได้อย่างถูกต้อง	4.37	0.77	มากที่สุด
5	ความถูกต้องและแม่นยำในการป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์ที่ทำงานแบบเรียลไทม์	4.21	0.80	มากที่สุด
ค่าเฉลี่ยรวม		4.22	0.80	มากที่สุด

ตารางที่ 4.12 ผลการประเมินด้านการทำงานได้ตามฟังก์ชันงานของระบบ

ข้อที่	ข้อความถาม	ผลการประเมิน		
		$\bar{X}$	S.D.	แปลผล
1	ความสามารถในการเชื่อมโยงข้อมูลกับระบบอินเทอร์เน็ตประสานสรรพสิ่ง	4.31	0.65	มากที่สุด
2	ความสามารถในการจัดการข้อมูล Log System ได้ถูกต้อง	4.34	0.77	มากที่สุด
3	ความสามารถในการจัดการแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย	4.34	0.77	มากที่สุด
4	ความสามารถในการจัดการป้องกันเครื่องคอมพิวเตอร์แม่ข่าย	4.34	0.73	มากที่สุด
5	ความสามารถในการจัดการประมวลผลได้อย่างเรียลไทม์	4.28	0.81	มากที่สุด
ค่าเฉลี่ยรวม		4.32	0.75	มากที่สุด

ตารางที่ 4.13 ผลการประเมินด้านความง่ายต่อการใช้งานระบบ

ข้อที่	ข้อความ	ผลการประเมิน		
		$\bar{X}$	S.D.	แปลผล
1	รูปแบบการใช้งานระบบ มีความเข้าใจง่ายในการเข้าถึงข้อมูล	4.38	0.69	มากที่สุด
2	ขั้นตอนการใช้งานง่าย เมนูไม่ซับซ้อน	4.25	0.72	มากที่สุด
3	ความเหมาะสมในการวางตำแหน่งของส่วนประกอบบนจอภาพ	4.31	0.72	มากที่สุด
4	ระบบมีความเหมาะสมที่จะใช้ในหน่วยงานของท่าน	4.19	0.83	มากที่สุด
5	ระบบมีความเหมาะสมที่จะนำไปปรับใช้กับ SME	4.32	0.76	มากที่สุด
ค่าเฉลี่ยรวม		4.29	0.74	มากที่สุด

ตารางที่ 4.14 ผลการประเมินด้านประสิทธิภาพการทำงานของระบบ

ข้อที่	ข้อความ	ผลการประเมิน		
		$\bar{X}$	S.D.	แปลผล
1	ความสามารถในการใช้งานและบันทึกข้อมูลของ Log System	4.46	0.70	มากที่สุด
2	ความสามารถของระบบในส่วนของการบันทึกข้อมูล	4.26	0.78	มากที่สุด
3	ความสามารถของระบบในส่วนของการแก้ไขเงื่อนไขการป้องกันภัยคุกคามทางไซเบอร์	4.25	0.87	มากที่สุด
4	ความสามารถของระบบในส่วนของการป้องกันการลบข้อมูล	4.35	0.71	มากที่สุด
5	ความสามารถของระบบในส่วนของการแสดงผลข้อมูล	4.57	0.58	มากที่สุด
ค่าเฉลี่ยรวม		4.38	0.73	มากที่สุด

ตารางที่ 4.15 ผลการประเมินด้านความมั่นคงปลอดภัยของระบบ

ข้อที่	ข้อคำถาม	ผลการประเมิน		
		$\bar{X}$	S.D.	แปลผล
1	ความเหมาะสมในการกำหนดสิทธิ์ของผู้ใช้ได้ตามหน้าที่	4.63	0.62	มากที่สุด
2	มีระบบ Login / Logout เพื่อตรวจสอบผู้เข้าใช้ระบบ	4.50	0.63	มากที่สุด
3	มีระบบการเข้ารหัสและถอดรหัสเพื่อส่งผ่านข้อมูลระหว่างหน้าจอ	4.41	0.58	มากที่สุด
4	มีกลไกการเปลี่ยนรหัสผู้ใช้งานให้มีความมั่นคงปลอดภัยไซเบอร์ภายในระบบ	4.40	0.72	มากที่สุด
5	ความเหมาะสมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบ	4.49	0.63	มากที่สุด
ค่าเฉลี่ยรวม		4.49	0.64	มากที่สุด

ตารางที่ 4.16 ผลรวมการประเมินความพึงพอใจในแต่ละด้าน

ข้อที่	ด้านของระบบ	ผลการประเมิน		
		$\bar{X}$	S.D.	แปลผล
1	ด้านระบบตรงกับความต้องการของผู้ใช้	4.22	0.80	มากที่สุด
2	ด้านการทำงานได้ตามฟังก์ชันงานของระบบ	4.32	0.75	มากที่สุด
3	ด้านความง่ายต่อการใช้งานระบบ	4.29	0.74	มากที่สุด
4	ด้านประสิทธิภาพการทำงานของระบบ	4.38	0.73	มากที่สุด
5	ด้านความมั่นคงปลอดภัยของระบบ	4.49	0.64	มากที่สุด
ค่าเฉลี่ยรวม		4.34	0.64	มากที่สุด

จากตารางที่ 4.16 ผลการประเมินความพึงพอใจในแต่ละด้าน ต่อการใช้งานระบบ SIEMKIT สำหรับการประเมินระบบป้องกัน และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ มีความ

เหมาะสม และยอมรับอยู่ในระดับ ระดับความพึงพอใจมากที่สุด โดยมีค่าเฉลี่ย 4.34 และส่วนเบี่ยงเบนมาตรฐาน 0.64 ($\bar{X}$ = 4.34, S.D. = 0.64) และเป็นการตอบสนองมติฐานข้อที่ (3) การประเมินระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ มีความเหมาะสมและยอมรับอยู่ในระดับมากที่สุด เมื่อพิจารณาความพึงพอใจผู้ใช้แต่ละประเด็นจำนวน 5 ประเด็นมีรายละเอียดดังต่อไปนี้

ประเด็นที่ 1 ด้านระบบตรงกับความต้องการของผู้ใช้ ระดับความพึงพอใจมากที่สุด มีค่าเฉลี่ย 4.22 ส่วนเบี่ยงเบนมาตรฐาน 0.80 ($\bar{X}$ = 4.22, S.D. = 0.80)

ประเด็นที่ 2 ด้านการทำงานได้ตามฟังก์ชันงานของระบบ ระดับความพึงพอใจมากที่สุด มีค่าเฉลี่ย 4.32 ส่วนเบี่ยงเบนมาตรฐาน 0.75 ($\bar{X}$ = 4.32, S.D. = 0.75)

ประเด็นที่ 3 ด้านความง่ายต่อการใช้งานระบบ ระดับความพึงพอใจมากที่สุด มีค่าเฉลี่ย 4.29 ส่วนเบี่ยงเบนมาตรฐาน 0.74 ($\bar{X}$ = 4.29, S.D. = 0.74)

ประเด็นที่ 4 ด้านประสิทธิภาพการทำงานของระบบ ระดับความพึงพอใจมากที่สุด มีค่าเฉลี่ย 4.38 ส่วนเบี่ยงเบนมาตรฐาน 0.73 ($\bar{X}$ = 4.38, S.D. = 0.73)

ประเด็นที่ 5 ด้านความมั่นคงปลอดภัยของระบบ ระดับความพึงพอใจมากที่สุด มีค่าเฉลี่ย 4.49 ส่วนเบี่ยงเบนมาตรฐาน 0.64 ($\bar{X}$ = 4.49, S.D. = 0.64)

4.4 ผลการนำเสนอแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ใหม่ที่เหมาะสมกับองค์กร ภายใต้ฐานความคิดที่ไม่ไว้วางใจใคร หากแต่ต้องตรวจสอบอยู่เสมอ

ผลการวิจัย แนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ใหม่เพื่อให้เหมาะสมกับองค์กรในยุคที่ข้อมูลและเทคโนโลยีเป็นสิ่งที่สำคัญอย่างยิ่ง โดยต้องพึงระวังซึ่งยึดถือฐานความคิดที่ไม่ไว้วางใจใคร และต้องมีการตรวจสอบอยู่เสมอหรือ Zero Trust Security Framework เป็นส่วนสำคัญของกระบวนการดังกล่าว ดังนั้น แนวทางในการออกแบบที่มีความมั่นคงปลอดภัยในสถาปัตยกรรมไซเบอร์ใหม่ขององค์กรมีดังต่อไปนี้

4.4.1 การออกแบบสถาปัตยกรรมเพื่อความมั่นคงปลอดภัยไซเบอร์ขององค์กร แบบใหม่

การออกแบบนั้นต้องมีการศึกษาความเข้าใจในเรื่องมาตรฐานและ Framework ต่าง ๆ และแนวปฏิบัติที่ดี จากมาตรฐานต่างๆ ดังต่อไปนี้เพื่อให้ทราบถึงหลักการและวัตถุประสงค์ก่อนนำไปปรับ

ใช้ หรือเป็นแนวคิดการ ออกแบบใหม่เพื่อให้คำนึงถึงความปลอดภัยและความมั่นคงของเครื่องคอมพิวเตอร์แม่ข่าย โดยผู้วิจัยได้สรุปไว้ดังนี้

1. NIST Cybersecurity Framework 2.0

NIST Cybersecurity Framework 2.0 (NIST CSF 2.0) เป็นมาตรฐานที่พัฒนาโดย National Institute of Standards and Technology (NIST) ของสหรัฐอเมริกา มีวัตถุประสงค์เพื่อช่วยองค์กรทุกขนาดในการจัดการและลดความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ โดย Framework นี้มีองค์ประกอบหลัก 5 ส่วน คือ Identify, Protect, Detect, Respond และ Recover ซึ่งเป็นขั้นตอนที่จำเป็นในการจัดการความเสี่ยงไซเบอร์ให้มีประสิทธิภาพ

2. Zero Trust Framework

Zero Trust เป็นแนวคิดด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ถือว่าไม่เชื่อถืออะไรเลย ไม่ว่าจะอยู่ในหรือนอกเครือข่ายขององค์กร โดยเน้นการตรวจสอบอย่างต่อเนื่อง การตรวจสอบตัวตนของผู้ใช้ และการจำกัดสิทธิ์ในการเข้าถึงข้อมูลและระบบขององค์กร แนวคิดนี้จะช่วยลดความเสี่ยงที่มาจากภัยคุกคามทั้งภายในและภายนอก

3. Security Mesh

Security Mesh คือแนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่เน้นการรวมและการจัดการเครื่องมือและบริการความมั่นคงปลอดภัยในลักษณะที่มีการกระจายตัว ไม่ใช่การรวมศูนย์แบบเดิม Security Mesh ทำให้สามารถสร้างระบบรักษาความมั่นคงปลอดภัยที่ยืดหยุ่นและสามารถปรับตัวตามความต้องการขององค์กรได้ โดยมีการเชื่อมต่อและการสื่อสารระหว่างโหนดต่าง ๆ ในระบบอย่างมีประสิทธิภาพ ทำให้สามารถตอบสนองต่อภัยคุกคามได้รวดเร็วและมีความแม่นยำสูงขึ้น ช่วยให้องค์กรสามารถปกป้องข้อมูลและสินทรัพย์ดิจิทัลได้ดียิ่งขึ้นในสภาพแวดล้อมที่มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว

4. COBIT 2019

COBIT 2019 เป็น Framework สำหรับการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศ (IT Governance and Management) ที่พัฒนาโดย ISACA โดยมีวัตถุประสงค์เพื่อช่วยให้องค์กรสามารถจัดการและควบคุมการใช้ไอที ให้สอดคล้องกับเป้าหมายและวัตถุประสงค์ทางธุรกิจ

COBIT 2019 มีการปรับปรุงจากรุ่นก่อนหน้าเพื่อให้ทันสมัยกับเทคโนโลยีและแนวปฏิบัติใหม่ ๆ รวมถึงเน้นการบริหารความเสี่ยงและการสร้างมูลค่าจากไอที

5. CIS Critical Security Controls (CIS Controls)

CIS Critical Security Controls (CIS Controls) เป็นชุดแนวทางปฏิบัติที่พัฒนาโดย Center for Internet Security (CIS) เพื่อช่วยองค์กรในการป้องกันภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ CIS Controls ประกอบด้วย 18 ข้อควรปฏิบัติที่ครอบคลุมการจัดการและการควบคุมความมั่นคงปลอดภัยของระบบสารสนเทศ เช่น การควบคุมการเข้าถึง การบริหารจัดการสินทรัพย์ การป้องกันมัลแวร์ และการรักษาความมั่นคงปลอดภัยเครือข่าย โดยมุ่งเน้นที่การลดความเสี่ยงและการเพิ่มประสิทธิภาพในการป้องกันและตอบสนองต่อเหตุการณ์ทางไซเบอร์ CIS Controls ได้รับการยอมรับอย่างกว้างขวางในอุตสาหกรรมและมีการอัปเดตเพื่อให้สอดคล้องกับภัยคุกคามที่เปลี่ยนแปลงไปอย่างต่อเนื่อง

6. ISO/IEC 27001

ISO/IEC 27001 เป็นมาตรฐานสากลสำหรับการจัดการความมั่นคงปลอดภัยของข้อมูล (Information Security Management System - ISMS) โดยมุ่งเน้นที่การปกป้องข้อมูลผ่านการประเมินความเสี่ยงและการนำมาตรการควบคุมที่เหมาะสมมาใช้ มาตรฐานนี้ครอบคลุมทุกแง่มุมของความมั่นคงปลอดภัยข้อมูล ตั้งแต่การประเมินความเสี่ยง การจัดการการเข้าถึง การเข้ารหัส การบำรุงรักษาความมั่นคงปลอดภัยทางกายภาพ และการบริหารจัดการเหตุการณ์ เพื่อให้มั่นใจว่าข้อมูลมีความมั่นคงปลอดภัยทั้งในแง่ของความลับ (confidentiality) ความถูกต้อง (integrity) และความพร้อมใช้งาน (availability) มาตรฐานนี้ได้รับการยอมรับในระดับสากลและสามารถนำไปใช้ได้กับองค์กรทุกขนาดและทุกประเภท

7. ISO/IEC 27002

ISO/IEC 27002 เป็นมาตรฐานที่ให้แนวทางสำหรับการจัดการความมั่นคงปลอดภัยของข้อมูลโดยเสนอแนะแนวปฏิบัติที่ดีที่สุดในการเลือกและใช้มาตรการควบคุมความมั่นคงปลอดภัยทางข้อมูล มาตรฐานนี้ออกแบบมาเพื่อช่วยองค์กรในการสร้างและรักษาระบบการจัดการความมั่นคงปลอดภัยของข้อมูล (ISMS) ที่มีประสิทธิภาพ โดยครอบคลุมด้านต่าง ๆ เช่น นโยบายความมั่นคงปลอดภัย การจัดการสินทรัพย์ ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม การจัดการการเข้าถึง

และการรักษาความมั่นคงปลอดภัยของข้อมูล ทั้งนี้เพื่อป้องกันการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาตและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

ทั้ง 7 หัวข้อนี้เป็นองค์ประกอบสำคัญในการเสริมสร้างความมั่นคงปลอดภัยและการบริหารจัดการทางเทคโนโลยีสารสนเทศที่มีประสิทธิภาพในองค์กรเป็นไปตามมาตรฐานสากลซึ่งได้สรุปเปรียบเทียบตามตารางที่ 4.17

ตารางที่ 4.17 สรุปเปรียบเทียบการกำกับด้านต่างๆ ของ Framework และ Standard

ด้านที่กำกับ	Framework/Standard						
	NIST Cybersecurity Framework 2.0	Zero Trust Framework	Security Mesh Framework	COBIT 2019	CIS Critical Security Controls	ISO 27001	ISO 27002
การจัดการและลดความเสี่ยง	✓	✓		✓	✓	✓	✓
การป้องกันอย่างมีประสิทธิภาพ	✓					✓	✓
วิเคราะห์ต่อเหตุการณ์	✓						
การตรวจจับและตอบสนองต่อเหตุการณ์	✓	✓	✓		✓		
การกู้คืนอย่างมีประสิทธิภาพ	✓					✓	
การควบคุมการเข้าถึง		✓	✓		✓	✓	

ตารางที่ 4.17 สรุปเปรียบเทียบการกำกับด้านต่างๆ ของ Framework และ Standard (ต่อ)

ด้านที่โดดเด่น	Framework/Standard						
	NIST Cybersecurity Framework 2.0	Zero Trust Framework	Security Mesh Framework	COBIT 2019	CIS Critical Security Controls	ISO 27001	ISO 27002
การบริหาร และรักษา ประสิทธิภาพ			✓	✓		✓	✓
การสนับสนุน ทางธุรกิจ				✓			
การตรวจสอบ และการ ปรับปรุงรักษา						✓	
การรักษา ความมั่นคง ปลอดภัยของ ข้อมูล			✓			✓	✓

เมื่อวิเคราะห์จากด้านต่างๆ ตามตารางที่ 4.17 จะเห็นว่าแต่ละ Framework และ Standard นั้นมีการมองเห็นที่เหมือนกันคือในด้านความมั่นคงปลอดภัยแต่จะมีส่วนต่างๆ ที่อาจจะแตกต่างกัน เพื่อนำไปปรับใช้เพื่อให้เกิดประสิทธิภาพเหมาะสมแต่ละองค์กร ซึ่งจากงานเขียนของ Jeffrey S. Zanzig (2022) เกี่ยวกับการการใช้ NIST Framework และ COBIT 2019 ในการนำเสนอบริการให้คำปรึกษาและการประกันความมั่นคงปลอดภัยทางไซเบอร์ ได้ให้สรุปว่า การประมวลผลข้อมูลในสภาพแวดล้อมทางไซเบอร์ก่อให้เกิดความเสี่ยงเช่นการละเมิดข้อมูลและแรนซัมแวร์ ทำให้ความต้องการความมั่นคง

ปลอดภัยทางไซเบอร์ เช่น NIST Framework สำหรับการชี้แนะองค์กรเกี่ยวกับมาตรการความมั่นคงปลอดภัยทางไซเบอร์

โดยงานวิจัยของ Scott Rose, Oliver Borchert, Stu Mitchell และ Sean Connelly (2020) มีความเห็นเกี่ยวกับ Zero Trust Architecture เป็นกระบวนการความมั่นคงปลอดภัยของเครือข่ายที่มุ่งเน้นไปที่ทรัพยากรแต่ละส่วน เพื่อควบคุมการเข้าถึงบริการบนคลาวด์ที่ไม่ได้อยู่ภายในขอบเขตเครือข่ายขององค์กร โมเดลการปรับใช้ Zero Trust Architecture เป็นต้น

จากศึกษางานวิจัยของ Donald L. Buresh (2022) เกี่ยวกับหลักปฏิบัติของปัญหาการทำงานระยะไกลและการละเมิดของ SolarWinds โดยใช้กรอบการป้องกันภัยคุกคาม ISO/IEC 27001 และข้อแนะนำ ISO/IEC 27002 ได้ชี้ให้เห็นถึงความซับซ้อนและความสำคัญของการจัดการความเสี่ยงทางไซเบอร์ที่เพิ่มขึ้นจากการทำงานระยะไกล โดยเฉพาะในสถานการณ์ที่มีการบุกรุกและการละเมิดเช่นที่เกิดขึ้นกับ SolarWinds ที่มีผลกระทบต่อภาพรวมของความมั่นคงปลอดภัยของไซเบอร์ทั่วโลก โดยการนำ ISO/IEC 27001 Cybersecurity Framework เป็นเครื่องมือในการจัดการความเสี่ยงทางไซเบอร์และ ISO/IEC 27002 Guidelines เป็นแนวทางในการปฏิบัติที่ถูกต้อง เป็นการนำการเรียนรู้จากเหตุการณ์เหล่านี้เพื่อปรับปรุงและเสริมความมั่นคงปลอดภัยของระบบและข้อมูลขององค์กรให้มีความมั่นคงปลอดภัยได้มากยิ่งขึ้น

อย่างไรก็ตาม สำหรับการออกแบบ Proposed Zero Trust Security Architecture ตามจุดประสงค์ที่ 4 ได้ดำเนินการนำหลักการที่กล่าวขึ้นมาข้างต้น มาปรับใช้ทั้ง 8 ส่วน โดยให้การควบคุมครอบคลุมตั้งแต่กระบวนการเข้าถึงเฉพาะผู้มีสิทธิการเข้าถึง ตรวจสอบสิทธิและความถูกต้อง ตรวจสอบการไหลของข้อมูลที่เกิดขึ้นตลอดเวลา ควบคุมการเข้าถึงเฉพาะส่วนที่ใช้งานพร้อมตรวจสอบอยู่เสมอและการเข้ารหัสข้อมูลในการเชื่อมต่อระหว่างผู้ใช้งานและสินทรัพย์ ระบุขอบเขตของสินทรัพย์ขององค์กรเพื่อจำกัดการเข้าถึง รวบรวมข้อมูลกิจกรรมต่างๆ ที่เกิดขึ้นขณะใช้งานสินทรัพย์ เปรียบเทียบตรวจสอบทานเงื่อนไขที่กำหนดเพื่อการป้องกันการโจมตี จนนำมาสู่การสร้างแนวทางเชิงนโยบายเพื่อให้เกิดการปฏิบัติที่ถูกต้องและสอดคล้องกับมาตรฐานการควบคุมที่เป็นสากล จนนำไปสู่การออกแบบ ออกแบบ Proposed Zero Trust Security Architecture แบบใหม่ จากนั้นได้นำการออกแบบและคำอธิบายในส่วนต่างๆ ให้ผู้ทรงคุณวุฒิทราบถึงรายละเอียด เพื่อทำการประเมินความ

1. Endpoint (อุปกรณ์ปลายทาง) คือ การกำหนดให้อุปกรณ์ที่เข้าใช้งานต้องได้รับความยินยอมให้สามารถเข้าสู่ภายในระบบได้หรือมีความน่าเชื่อถือสามารถควบคุมให้เป็นมาตรฐานขององค์กรโดยได้ลงทะเบียนไว้กับองค์กรเรียบร้อยแล้ว

2. User & Password (ชื่อผู้ใช้และรหัสผ่าน) คือ การกำหนดรหัสผ่านตามหลัก Zero Trust นั้นมีหลายขั้นตอนและรวมถึงเงื่อนไขที่สำคัญที่ต้องปฏิบัติตาม เพื่อให้ระบบรักษาความมั่นคงปลอดภัยได้อย่างเต็มที่ ในการกำหนดรหัสผ่านตามหลัก Zero Trust ได้แก่

2.1 ความแข็งแกร่งของรหัสผ่าน คือ รหัสผ่านควรมีความยาวพอสมควรและมีความซับซ้อน เช่น การผสมตัวอักษรตัวพิมพ์ใหญ่และตัวเล็ก ตัวเลข และสัญลักษณ์พิเศษ เพื่อลดความเป็นไปได้ที่จะถูกทำลายโดยการโจมตีด้วยวิธีการคำนวณ

2.2 การเปลี่ยนรหัสผ่าน คือ ระบบควรบังคับให้ผู้ใช้เปลี่ยนรหัสผ่านอย่างสม่ำเสมอ เช่น ทุก 30 วันหรือตามนโยบายขององค์กร

2.3 การไม่ใช้รหัสผ่านที่เข้ามาแล้ว คือ ระบบควรไม่อนุญาตให้ใช้รหัสผ่านที่เคยใช้มาแล้ว เพื่อป้องกันการโจมตีด้วยวิธีการสุ่มลองครั้งหลังจากที่รหัสผ่านถูกเปิดเผย

2.4 การใช้ Multi-factor Authentication (MFA) คือ การใช้ MFA เพื่อเพิ่มชั้นความมั่นคงปลอดภัยโดยใช้วิธีการตรวจสอบตัวตนมากกว่าหนึ่งวิธี เช่น การใช้รหัสผ่านพร้อมกับรหัสยืนยันที่ถูกส่งไปยังโทรศัพท์เคลื่อนที่หรืออีเมล

3. Identity and Access Management (IAM) คือ กระบวนการหรือระบบที่ใช้ในการจัดการและควบคุมการเข้าถึงทรัพยากรต่างๆ ในระบบขององค์กร โดยมุ่งเน้นไปที่การรับรองตัวตนของผู้ใช้และการควบคุมสิทธิการเข้าถึง เพื่อให้แน่ใจว่าเฉพาะผู้ที่มีสิทธิ์และเป็นผู้ยืนยันตัวตนได้เท่านั้นที่สามารถเข้าถึงข้อมูลและทรัพยากรได้ในองค์กร โดย IAM มักมีความสำคัญในระบบ IT และความมั่นคงปลอดภัยข้อมูล เป็นส่วนหนึ่งของการดำเนินงานที่ปลอดภัยและมีประสิทธิภาพขององค์กร ฟังก์ชันหลักของ Identity and Access Management ประกอบด้วย

3.1 Authentication (การรับรองตัวตน) คือ การช่วยให้ระบบสามารถรับรองตัวตนของผู้ใช้ได้ โดยใช้หลายวิธี เช่น รหัสผ่าน การใช้งานบัตรประจำตัว หรือการใช้งานช่องสัญญาณไร้สาย (Biometrics) เพื่อให้แน่ใจว่าผู้ใช้คือผู้ที่ได้รับอนุญาตและยืนยันตัวตนได้

3.2 Authorization (การอนุญาต) คือ การกำหนดสิทธิ์และการเข้าถึงทรัพยากรของระบบ โดยกำหนดสิทธิ์ของผู้ใช้ตามบทบาทหรือกลุ่มของผู้ใช้ ซึ่งช่วยให้แน่ใจว่าผู้ใช้งานมีการเข้าถึงเฉพาะข้อมูลและทรัพยากรที่เป็นไปตามนโยบายและความเหมาะสม

3.3 Administration (การบริหารจัดการ) คือ การช่วยให้ผู้ดูแลระบบสามารถจัดการข้อมูลผู้ใช้ บทบาท และสิทธิ์การเข้าถึงได้อย่างมีประสิทธิภาพ รวมถึงการสร้าง การแก้ไข และการลบบัญชีผู้ใช้ การกำหนดสิทธิ์ และการจัดการข้อมูลอื่นๆ ที่เกี่ยวข้อง

3.4 Audit and Compliance (การตรวจสอบและความเป็นไปได้) เป็นส่วนช่วยให้สามารถตรวจสอบการเข้าถึงข้อมูลและทรัพยากร รวมถึงบันทึกกิจกรรมหรือเหตุการณ์การเข้าถึงเพื่อให้ปฏิบัติตามกฎระเบียบและมาตรฐานความมั่นคงปลอดภัย

3.5 Integration (การผสมผสาน) คือ การทำให้ระบบสามารถผสมผสานกับแอปพลิเคชันและระบบอื่นๆ ในองค์กรได้อย่างสมบูรณ์ เพื่อให้การจัดการตัวตนและการเข้าถึงทรัพยากรเป็นไปอย่างเรียบร้อยและมีประสิทธิภาพโดยรวมแล้ว Identity and Access Management (IAM) เป็นกลไกสำคัญที่ช่วยให้องค์กรสามารถจัดการและควบคุมการเข้าถึงทรัพยากรได้อย่างมีประสิทธิภาพและปลอดภัย

4. Traffic (ข้อมูลการจราจร) การตรวจสอบและการตอบสนองทันทีต่อการจราจรและการเข้าถึงข้อมูลที่ไม่ถูกต้องหรือไม่เหมาะสมเป็นสิ่งสำคัญอย่างมากในสภาพแวดล้อมด้านความมั่นคงปลอดภัยของเครือข่ายอินเทอร์เน็ตและระบบสารสนเทศอื่นๆ การเรียกใช้เทคโนโลยีการตรวจจับการบุกรุกและการจำกัดการเข้าถึงเป็นวิธีที่สำคัญในการตรวจสอบและป้องกันการบุกรุกจากบุคคลที่ไม่พึงประสงค์หรือการเข้าถึงทรัพยากรที่ไม่ได้รับอนุญาต ด้วยการใช้เทคโนโลยีนี้ ระบบสามารถตรวจจับการกระทำที่ไม่เหมาะสมหรือเกินกำหนดได้ทันที และมีการตอบสนองทันทีโดยการจำกัดหรือบล็อกการเข้าถึงทรัพยากรที่เสี่ยงต่อความมั่นคงปลอดภัย นอกจากนี้ การตรวจสอบและการตอบสนองเหล่านี้มักจะเป็นเรื่องแม่นยำและอัตโนมัติในโหมดเรียลไทม์ เพื่อให้ระบบสามารถรับมือกับสถานการณ์ที่เปลี่ยนแปลงอย่างรวดเร็วและป้องกันอันตรายในเวลาที่เกิดขึ้นในทันทีทันใด การป้องกันอุบัติเหตุและการลดความเสี่ยงเป็นสิ่งสำคัญเพื่อให้ระบบทำงานอย่างมีประสิทธิภาพและมั่นคงในการให้บริการข้อมูลแก่ผู้ใช้งาน ในทางปฏิบัติ การใช้เทคโนโลยีการตรวจจับการบุกรุกและการจำกัดการเข้าถึงช่วยให้

เครือข่ายและระบบสารสนเทศปลอดภัยและเสถียรภาพมากขึ้นในการดำเนินงานประจำวันขององค์กร และธุรกิจ

5. Control (การควบคุม) คือ การควบคุมแบบ Zero Trust เน้นการใช้นโยบายที่เข้มงวดและการควบคุมการเข้าถึงทรัพยากรอย่างเป็นระบบ โดยไม่ไว้วางใจตามหน้าที่หรือเครือข่ายที่ผู้ใช้งานจนถึงอุปกรณ์ที่ใช้เชื่อมต่อ โดยวิธีการควบคุมและปกป้องข้อมูลในรูปแบบ Zero Trust ดังนี้

5.1 Real-time Control (ควบคุมแบบเรียลไทม์) คือ การควบคุมการเข้าถึงทรัพยากรอยู่ตลอดเวลาและเฉพาะที่จำเป็นสำหรับการปฏิบัติงาน Principle of Least Privilege (POLP) โดยใช้ข้อมูลเกี่ยวกับตัวตนของผู้ใช้งาน มากำหนดสิทธิ์การเข้าถึง Identity-Based Access Control (IBAC) ด้วยเงื่อนไขต่างๆ Attribute-Based Access Control (ABAC) เช่น ตำแหน่ง หน้าที่ บทบาท และความสัมพันธ์ ในการกำหนดสิทธิ์

5.2 Classification (การจัดหมวดหมู่ข้อมูล) เช่น การจัดหมวดหมู่ข้อมูลตามความลับและความเสี่ยง (Data Sensitivity Classification) เพื่อให้สามารถใช้นโยบายการเข้าถึงที่เข้มงวดและเชิงรุกภายในองค์กร กำหนดนโยบายในการจัดการข้อมูลตลอดจนถึงการทำลายข้อมูลในขั้นตอนการบริหารจัดการวงจรชีวิตของข้อมูล (Data Lifecycle Management)

5.3 Encryption (การเข้ารหัส) เช่น เข้ารหัสข้อมูลที่กำลังถูกส่งผ่านเครือข่าย (Data Encryption in Transit) เช่น การใช้ SSL/TLS สำหรับการเชื่อมต่อที่ปลอดภัย เข้ารหัสข้อมูลที่อยู่ในการเก็บบันทึกหรือฐานข้อมูล (Data Encryption at Rest) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

การควบคุมและป้องกันข้อมูลแบบ Zero Trust ช่วยให้องค์กรมีการควบคุมและความมั่นคงปลอดภัยที่เหมาะสมต่อการเข้าถึงข้อมูล โดยไม่ไว้วางใจตามแหล่งกำเนิดของข้อมูลหรือตำแหน่งที่มาของผู้ใช้หรืออุปกรณ์ นอกจากนี้ยังช่วยให้สามารถป้องกันการบุกรุกและการรั่วไหลข้อมูลได้อย่างมีประสิทธิภาพและมั่นคง

6. Assets (สินทรัพย์) คือ การจัดการทรัพยากรหรือ Assets แบบ Zero Trust เน้นการรับรองและควบคุมการเข้าถึงสินทรัพย์ทุกอย่างเคร่งครัด โดยไม่ไว้วางใจตามหน้าที่หรือเครือข่าย แนวคิดและวิธีการที่ใช้ในการจัดการสินทรัพย์ในรูปแบบ ดังนี้

6.1 การระบุและการจำแนกประเภทของสินทรัพย์ (Asset Identification and Classification) ระบุและจำแนกประเภทของสินทรัพย์ที่สำคัญตามลักษณะของแต่ละสินทรัพย์ เช่น ข้อมูลที่ละเอียด ระบบ เซิร์ฟเวอร์ และแอปพลิเคชัน

6.2 การตั้งค่านโยบายการเข้าถึง (Access Policy Setting) กำหนดนโยบายการเข้าถึงทรัพยากรอย่างเข้มงวดและโดยใช้หลักการ Zero Trust เพื่อให้มั่นใจว่าเฉพาะผู้ที่มีสิทธิ์เท่านั้นที่สามารถเข้าถึงได้

6.3 การใช้งานบัตรระบบและการส่งข้อมูลโดยใช้การเข้ารหัส (Tokenization and Encryption) ใช้งานบัตรผ่านบนระบบเพื่อรับรองตัวตนและใช้การเข้ารหัสข้อมูลเพื่อป้องกันการถูกแอบดักจับข้อมูลขณะการส่งผ่าน

6.4 การตรวจสอบและการวิเคราะห์ (Monitoring and Analysis) คือ การตรวจสอบและวิเคราะห์การเข้าถึงสินทรัพย์โดยตลอดเวลา เพื่อตรวจจับและตอบสนองต่อกิจกรรมที่ไม่ปกติ

6.5 การใช้งาน Identity and Access Management (IAM) คือ การใช้ระบบ IAM เพื่อจัดการตัวตนและการเข้าถึงของผู้ใช้ โดยใช้หลักการ Zero Trust เพื่อควบคุมการเข้าถึงสินทรัพย์

6.6 การสร้างและการบริหารจัดการนโยบาย (Policy Creation and Management) คือ การสร้างและบริหารจัดการนโยบายการเข้าถึงทรัพยากรที่เข้มงวดและเชื่อถือได้ตามหลักการ Zero Trust

6.7 การป้องกันและการตอบสนองต่อการบุกรุก (Prevention and Response to Intrusions) คือ การใช้มาตรการป้องกันและการตอบสนองต่อการบุกรุกอย่างรวดเร็วและมีประสิทธิภาพ เพื่อป้องกันและลดความเสี่ยงที่อาจเกิดขึ้น

การจัดการทรัพยากรแบบ Zero Trust ช่วยให้องค์กรมีความเชื่อมั่นในการควบคุมและความมั่นคงปลอดภัยของสินทรัพย์ที่สำคัญ โดยไม่วางใจตามหน้าที่หรือเครือข่าย และช่วยลดความเสี่ยงต่อการถูกบุกรุกหรือการรั่วไหลข้อมูลลงไปด้วย

7. SIEM คือการปรับใช้ SIEM (Security Information and Event Management) แบบ Zero Trust เน้นการตรวจสอบและวิเคราะห์ข้อมูลเกี่ยวกับความมั่นคงปลอดภัยและเหตุการณ์ที่เกิดขึ้นในระบบขององค์กรโดยใช้หลักการ Zero Trust เพื่อควบคุมและป้องกันการบุกรุกอย่างเฉพาะเจาะจง วิธีการปรับใช้ SIEM แบบ Zero Trust ดังนี้

7.1 การตรวจสอบและการวิเคราะห์โดยตลอดเวลา (Continuous Monitoring and Analysis) คือ ตรวจสอบและวิเคราะห์เหตุการณ์และกิจกรรมที่เกิดขึ้นในระบบขององค์กรอย่างต่อเนื่อง โดยใช้หลักการ Zero Trust เพื่อตรวจจับและตอบสนองต่อการบุกรุกที่เกิดขึ้นได้อย่างรวดเร็ว

7.2 การตรวจสอบเหตุการณ์ข้ามเครือข่าย (Cross-Network Event Correlation) คือ การตรวจสอบและวิเคราะห์เหตุการณ์ที่เกิดขึ้นทั้งภายในและภายนอกเครือข่าย โดยใช้ข้อมูลจากแหล่งที่มาต่างๆ เพื่อค้นหาและตอบสนองต่อภัยคุกคามที่เกิดขึ้นในทุกๆ มุมของระบบ

7.3 การใช้แนวทางการตอบสนองที่เชื่อถือได้ (Trusted Response Strategies) คือ การใช้แนวทางการตอบสนองต่อเหตุการณ์ที่ตรวจจับได้ โดยใช้วิธีการที่เชื่อถือได้และมีประสิทธิภาพ เพื่อรักษาความมั่นคงปลอดภัยของระบบ

7.4 การตรวจสอบและการตอบสนองต่อการละเมิดการเข้าถึงแบบ Real-time (Real-time Detection and Response) คือ การตรวจสอบและตอบสนองต่อการละเมิดอย่างรวดเร็วในขณะที่เหตุการณ์กำลังเกิดขึ้น เพื่อลดความเสี่ยงและความเสียหายที่อาจเกิดขึ้น

7.5 การสร้างและการบริหารจัดการนโยบาย (Policy Creation and Management) คือ การสร้างและบริหารจัดการนโยบายการตรวจสอบและการตอบสนองต่อภัยคุกคามโดยใช้หลักการ Zero Trust เพื่อให้มั่นใจว่าระบบมีการควบคุมและความมั่นคงปลอดภัยที่เหมาะสม

8. Policy คือ การปรับใช้นโยบายแบบ Zero Trust เน้นการจัดการและควบคุมความเชื่อมั่นและความมั่นคงปลอดภัยของข้อมูลและทรัพยากรในระบบองค์กร โดยไม่วางใจตามตำแหน่งหรือบริบทที่เกิดขึ้น ด้วยวิธีการปรับใช้แต่ละนโยบาย ดังนี้

8.1 Governance (กำกับดูแลการดำเนินงาน) คือ สร้างกรอบการบริหารการดำเนินงานที่มีเครื่องมือและกระบวนการเพื่อควบคุมการเข้าถึงข้อมูลและทรัพยากร โดยใช้หลักการ Zero Trust เพื่อให้มั่นใจว่าการบริหารการดำเนินงานเป็นไปอย่างมีประสิทธิภาพและปลอดภัย

8.2 Compliance (การปฏิบัติตามข้อบังคับ) คือ สร้างนโยบายการปฏิบัติตามข้อบังคับและมาตรฐานความมั่นคงปลอดภัยที่เกี่ยวข้อง โดยใช้หลักการ Zero Trust เพื่อให้การปฏิบัติตามข้อบังคับเป็นไปอย่างเข้มงวดและเชื่อถือได้

8.3 Security Assessment (การประเมินความมั่นคงปลอดภัย) คือ จัดทำการประเมินความมั่นคงปลอดภัยและการตรวจสอบเพื่อตรวจจับความเสี่ยงและช่องโหว่ในระบบ โดยใช้หลักการ Zero Trust เพื่อให้การประเมินความมั่นคงปลอดภัยเป็นไปอย่างอิสระและเชื่อถือได้

การปรับใช้นโยบายแบบ Zero Trust ในส่วนของ Governance, Compliance และ Security Assessment คือการช่วยให้องค์กรมีการควบคุมและมีความมั่นคงปลอดภัยต่อการเข้าถึงข้อมูลและทรัพยากร โดยไม่ไว้วางใจตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย ซึ่งช่วยให้สามารถปฏิบัติตามข้อบังคับและมาตรฐานความมั่นคงปลอดภัยได้อย่างน่าเชื่อถือ

4.4.2 การประเมินได้มีการสอบถามความคิดเห็นของผู้ทรงคุณวุฒิเกี่ยวกับความเหมาะสมและการยอมรับ ของ Proposed Zero Trust Security Architecture แบบใหม่ แบ่งออกเป็น 3 ส่วน คือ

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ทรงคุณวุฒิ

ข้อมูลทั่วไปของผู้ตอบแบบประเมินในครั้งนี้เป็นผู้ทรงคุณวุฒิที่ได้รับการแต่งตั้งจำนวน 6 ท่านมีรายละเอียดจากตารางที่ 4.18 ดังต่อไปนี้

ตารางที่ 4.18 ข้อมูลทั่วไปของผู้ทรงคุณวุฒิ

ลำดับ ที่	ชื่อ-สกุล	ตำแหน่ง	สถานที่ทำงาน	ประสบการณ์ ที่ทำงานด้าน เทคโนโลยี ดิจิทัล
1	ผศ.ดร.สุนิษา คิดใจเดียว	ประธานหลักสูตร สาขาวิชาเทคโนโลยี สารสนเทศและ นวัตกรรมดิจิทัล	มหาวิทยาลัยราชภัฏ นครศรีธรรมราช	มากกว่า 10 ปี
2	ผศ.ดร.สำราญ ไชยคำวัง	ผู้ช่วยศาสตราจารย์	มหาวิทยาลัยราชภัฏ เชียงราย	มากกว่า 10 ปี

ตารางที่ 4.18 ข้อมูลทั่วไปของผู้ทรงคุณวุฒิ (ต่อ)

ลำดับ ที่	ชื่อ-สกุล	ตำแหน่ง	สถานที่ทำงาน	ประสบการณ์ ที่ทำงานด้าน เทคโนโลยี ดิจิทัล
3	ผศ.ดร.ชัยพร ทบแป	ผู้จัดการศูนย์ นวัตกรรมดิจิทัล	บริษัท โทรคมนาคม แห่งชาติ จำกัด (มหาชน)	มากกว่า 10 ปี
4	ดร. เอกฉัตร บ่ายคล้อย	ประธานกรรมการ	บริษัท EP&IT Solution Co., Ltd.	มากกว่า 10 ปี
5	ดร. เทพฤทธิ์ พระเทพ	วิศวกรเทคโนโลยี ฝ่ายวิเคราะห์และ ออกแบบ	บริษัท NEYAA Inc. Group	มากกว่า 10 ปี
6	ดร. เกรียงไกร ภูวนิชย์	รองประธาน คณะกรรมการสาขา วิศวกรรมคอมพิวเตอร์	วิศวกรรมสถานแห่ง ประเทศไทยในพระ บรมราชูปถัมภ์ (วสท)	มากกว่า 10 ปี

ส่วนที่ 2 ความเหมาะสมและการยอมรับของ Proposed Zero Trust Security Architecture แบบใหม่สำหรับองค์กร ตามแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมกับองค์กร ภายใต้อาณัติความคิดที่ไม่ไว้ใจใคร หากแต่ต้องตรวจสอบอยู่เสมอ

การพัฒนา Proposed Zero Trust Security Architecture แบบใหม่ที่เหมาะสมกับองค์กร เพื่อใช้เป็นแนวทางในรับมือกับความเสี่ยงและภัยคุกคามทางไซเบอร์นั้น ผู้วิจัยได้ศึกษาและอ้างอิงจาก Framework ต่าง ๆ อาทิ NIST Cybersecurity 2.0, Zero Trust, Security Mech และ COBIT 2019 นอกจากนี้ ยังศึกษาแนวปฏิบัติที่ดี (Best Practice Guidelines) เช่น CIS Critical Security Controls จาก SANS Institute รวมทั้งมาตรฐานอื่น ๆ ได้แก่ ISO 27001 และ ISO 27002 เป็นต้น อย่างไรก็ตาม

Proposed Zero Trust Security Architecture แบบใหม่ ที่ผู้วิจัยได้พัฒนาขึ้นมานี้ จะมีองค์ประกอบ 8 ส่วน รายละเอียด ดังในภาพประกอบที่ 4.25 ดังนี้

การประเมินความเหมาะสมผู้วิจัยสร้างข้อคำถามเพื่อให้ผู้ทรงคุณวุฒิทำเครื่องหมาย ☒ ลงในช่องที่ตรงกับความจริง ความคิดเห็น หรือความรู้สึกของผู้ทรงคุณวุฒิมากที่สุดเพียงช่องเดียว แบ่งระดับคำตอบเป็น 5 ระดับ ดังนี้

- 5 หมายถึง เหมาะสมหรือเห็นด้วยมากที่สุด
- 4 หมายถึง เหมาะสมหรือเห็นด้วยมาก
- 3 หมายถึง เหมาะสมหรือเห็นด้วยปานกลาง
- 2 หมายถึง เหมาะสมหรือเห็นด้วยน้อย
- 1 หมายถึง เหมาะสมหรือเห็นด้วยน้อยที่สุด

ตารางที่ 4.19 ผลการประเมินประเด็นสอบถาม

ข้อที่	ประเด็นสอบถาม	ผลการประเมิน		
		$\bar{X}$	S.D.	แปลผล
1	Proposed Zero Trust Security Architecture แบบใหม่ ที่พัฒนาขึ้นมีความเหมาะสมกับการนำไปใช้งานในองค์กร	4.50	0.55	มากที่สุด
2	Proposed Zero Trust Security Architecture แบบใหม่ ที่พัฒนาขึ้นมีความครอบคลุมในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กร	4.50	0.84	มากที่สุด
3	Proposed Zero Trust Security Architecture แบบใหม่ที่พัฒนาขึ้น ไม่ซับซ้อนยุ่งยากมีความเข้าใจง่ายต่อการนำไปใช้ในองค์กร	4.50	0.84	มากที่สุด

ตารางที่ 4.19 ผลการประเมินประเด็นสอบถาม (ต่อ)

ข้อที่	ประเด็นสอบถาม	ผลการประเมิน		
		$\bar{x}$	S.D.	แปลผล
4	Proposed Zero Trust Security Architecture แบบใหม่ ที่พัฒนาขึ้น จะสามารถปรับปรุงระดับความพร้อมทางไซเบอร์และรับมือกับความเสี่ยงและภัยคุกคามทางไซเบอร์ในองค์กร	4.50	0.55	มากที่สุด
5	Proposed Zero Trust Security Architecture แบบใหม่ที่พัฒนาขึ้นสามารถพัฒนายกระดับขีดความสามารถและมาตรฐานความมั่นคงปลอดภัยไซเบอร์ขององค์กร	4.50	0.55	มากที่สุด

ผู้วิจัยนำแบบประเมินให้ผู้ทางคุณวุฒิทั้ง 6 ท่าน ทำการประเมินความเหมาะสมและการยอมรับของ Proposed Zero Trust Security Architecture แบบใหม่และเพื่อตอบสนองมาตรฐานการวิจัยที่ว่า แนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ใหม่ที่เหมาะสมกับองค์กร ภายใต้ฐานความคิดที่ไม่ไว้วางใจใคร หากแต่ต้องตรวจสอบอยู่เสมอ นั้นมีความเหมาะสมและการยอมรับอยู่ในระดับมาก โดยใช้แบบสอบถามประมาณค่า 5 ระดับ

โดยภาพรวมของผู้ตอบแบบสอบถามเห็นว่าความเหมาะสมและการยอมรับ Proposed Zero Trust Security Architecture แบบใหม่ ที่พัฒนาขึ้นมีความเหมาะสมกับการนำไปใช้งานในองค์กร ผู้ตอบแบบสอบถามได้ประเมินระดับความเหมาะสมและการยอมรับอยู่ในระดับ **เหมาะสมหรือเห็นด้วยมากที่สุด** ซึ่งเป็นไปตามสมมติฐานข้อที่ (4) แนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ใหม่ที่เหมาะสมกับองค์กร ภายใต้ฐานความคิดที่ไม่ไว้วางใจใคร หากแต่ต้องตรวจสอบอยู่เสมอ นั้นมีความเหมาะสมเป็นไปได้และการยอมรับอยู่ในระดับมาก อย่างไรก็ตามเมื่อพิจารณาทีละรายประเด็นพบว่า

1. Proposed Zero Trust Security Architecture แบบใหม่ ที่พัฒนาขึ้นมีความเหมาะสมกับการนำไปใช้งานในองค์กร ผู้ตอบแบบสอบถามมีระดับความเหมาะสมและการยอมรับอยู่ในระดับเหมาะสมหรือเห็นด้วยมากที่สุด ($\bar{X}$ = 4.50, S.D. = 0.55)

2. Proposed Zero Trust Security Architecture แบบใหม่ ที่พัฒนาขึ้นมีความครอบคลุมในการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กร ผู้ตอบแบบสอบถามมีระดับความเหมาะสมและการยอมรับอยู่ในระดับเหมาะสมหรือเห็นด้วยมากที่สุด ($\bar{X}$ = 4.50, S.D. = 0.84)

3. Proposed Zero Trust Security Architecture แบบใหม่ที่พัฒนาขึ้นไม่ซับซ้อนยุ่งยาก มีความเข้าใจง่ายต่อการนำไปใช้ในองค์กร ผู้ตอบแบบสอบถามมีระดับความเหมาะสมและการยอมรับอยู่ในระดับเหมาะสมหรือเห็นด้วยมากที่สุด ($\bar{X}$ = 4.50, S.D. = 0.84)

4. Proposed Zero Trust Security Architecture แบบใหม่ ที่พัฒนาขึ้นจะสามารถปรับปรุงระดับความพร้อมทางไซเบอร์และรับมือกับความเสี่ยงและภัยคุกคามทางไซเบอร์ในองค์กร ผู้ตอบแบบสอบถามมีระดับความเหมาะสมและการยอมรับอยู่ในระดับเหมาะสมหรือเห็นด้วยมากที่สุด ($\bar{X}$ = 4.50, S.D. = 0.55)

5. Proposed Zero Trust Security Architecture แบบใหม่ที่พัฒนาขึ้นสามารถพัฒนาระดับขีดความสามารถและมาตรฐานความมั่นคงปลอดภัยไซเบอร์ขององค์กร ผู้ตอบแบบสอบถามมีระดับความเหมาะสมและการยอมรับอยู่ในระดับเหมาะสมหรือเห็นด้วยมากที่สุด ($\bar{X}$ = 4.50, S.D. = 0.55)

ส่วนที่ 3 ระดับความคิดเห็นโดยรวมของผู้ทรงคุณวุฒิที่มีต่อ Proposed Zero Trust Security Architecture แบบใหม่ ตามแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ใหม่ที่เหมาะสมกับองค์กร ภายใต้ฐานความคิดที่ไม่ไว้ว่างใจใคร หากแต่ต้องตรวจสอบเสมอ

การประเมินความเหมาะสมและการยอมรับของ Proposed Zero Trust Security Architecture แบบใหม่ ตามแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ใหม่

ตารางที่ 4.20 ผลการประเมินระดับความเหมาะสมหรือการยอมรับ

ข้อที่	ประเด็นสอบถาม	ผลการประเมิน		
		$\bar{X}$	S.D.	แปลผล
1	ความเหมาะสม “Proposed Zero Trust Security Architecture แบบใหม่ ที่พัฒนาขึ้นตามแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมกับองค์กร ภายใต้ฐานความคิดที่ไม่ไว้วางใจใคร หากแต่ต้องตรวจสอบเสมอ”	4.67	0.52	เหมาะสมมากที่สุด
2	การยอมรับ “Proposed Zero Trust Security Architecture แบบใหม่ ที่พัฒนาขึ้นตามแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมกับองค์กร ภายใต้ฐานความคิดที่ไม่ไว้วางใจใคร หากแต่ต้องตรวจสอบเสมอ”	4.67	0.52	เหมาะสมมากที่สุด

1. “Proposed Zero Trust Security Architecture แบบใหม่ ที่พัฒนาขึ้นตามแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมกับองค์กร ภายใต้ฐานความคิดที่ไม่ไว้วางใจใคร หากแต่ต้องตรวจสอบเสมอ” ตามภาพประกอบที่ 4.25 มีความเหมาะสมอยู่ในระดับใด ผู้ตอบแบบสอบถามมีระดับความเหมาะสมอยู่ในระดับ **เหมาะสมมากที่สุด** ($\bar{X}=4.67$, S.D. = 0.52)

2. “Proposed Zero Trust Security Architecture แบบใหม่ ที่พัฒนาขึ้นตามแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมกับองค์กร ภายใต้ฐานความคิดที่ไม่ไว้วางใจใคร หากแต่ต้องตรวจสอบเสมอ” ผู้ตอบแบบสอบถามมีระดับการยอมรับอยู่ในระดับ **เหมาะสมมากที่สุด** ($\bar{X}=4.67$, S.D. = 0.52)

4.5 สรุป

ผลการวิจัยในครั้งนี้ได้ศึกษารวบรวม วิเคราะห์ข้อมูลภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับการ โจมตี Brute Force Attack เพื่อนำข้อมูลที่ได้มาเป็นแนวทางในการพัฒนาการวิเคราะห์ข้อมูลภัยคุกคามทางไซเบอร์ที่เกิดกับเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการเข้าถึงจากอินเทอร์เน็ต เพื่อเรียนรู้แนวทางการป้องกัน อีกทั้งการแจ้งเตือนไปยังผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายนั้น สามารถรับมือ หรือยับยั้งความเสียหายที่จะเกิดขึ้น ถ้าหากผู้ไม่หวังดีสามารถ เข้ายึดครองเครื่องคอมพิวเตอร์แม่ข่ายขององค์กรได้

4.5.1 ผลการวิจัยวัตถุประสงค์ข้อที่ 1 เพื่อทำการวิเคราะห์ภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายในองค์กร ผลการวิจัยพบว่า สามารถนำระบบ SIEM ไปปรับใช้ได้เพื่อเพิ่มความแข็งแกร่งต่อการป้องกันภัยคุกคามทางไซเบอร์ และง่ายต่อการวิเคราะห์เหตุการณ์ที่เกิดกับเครื่องคอมพิวเตอร์แม่ข่าย อีกทั้งยังสามารถระบุประเภทหรือขั้นตอนของภัยคุกคามนั้นๆ ว่าเป็นอย่างไร เพื่อเป็นการป้องกันหรือรับมือกับเหตุการณ์ที่จะเกิดขึ้นในอนาคต หรือใช้นำไปซึ่งการวิเคราะห์จุดอ่อนของการให้บริการเครื่องคอมพิวเตอร์แม่ข่าย ตามคู่มือการใช้งานระบบ SIEM ในภาคผนวก ข

4.5.2 ผลการวิจัยวัตถุประสงค์ข้อที่ 2 พัฒนาระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ ผลการวิจัยพบว่า กระประเมิน และวิเคราะห์การโจมตีได้อย่างถูกต้องจากเหตุการณ์ที่ได้ทำการบันทึกในระบบ SIEM และหาจุดที่มีความสัมพันธ์ระหว่างแต่ละข้อกำหนดในกฎ ของระบบ SIEM ก็จะสามารถนำมารวบรวมจัดกลุ่มใหม่เพื่อใช้ในการวิเคราะห์ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพมากขึ้นและครอบคลุมทุกกิจกรรมที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายที่องค์กรให้บริการอยู่

4.5.3 ผลการวิจัยวัตถุประสงค์ข้อที่ 3 เพื่อทำการประเมินประสิทธิภาพของระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย ผลการวิจัยพบว่า การป้องกัน และการแจ้งเตือนไปยังผู้ดูแลระบบแม่ข่ายมีความสำคัญหาก สามารถระบุการโจมตีได้แต่ไม่สามารถป้องกันได้ ก็จะทำให้ระบบการป้องกันต้องอาศัยมนุษย์ เข้ามาจัดการใดๆ ในแต่ละกิจกรรม ซึ่งภัยคุกคามในปัจจุบันสามารถเกิดขึ้นตลอดเวลา อ้างถึงการบันทึกในระบบ SIEMKIT ที่ผู้วิจัยได้ทำการบันทึกเหตุการณ์การที่เกิดกับเครื่องคอมพิวเตอร์แม่ข่ายภายใน 1 เดือนนั้นมีมากกว่า 2 หมื่นรายการ นั้น

สะท้อนให้เห็นว่าการป้องกัน หรือยับยั้งภัยคุกคามที่ใกล้เคียงเรียลไทม์ ยิ่งบ่งชี้ประสิทธิภาพการป้องกัน เครื่องคอมพิวเตอร์แม่ข่ายได้ดียิ่งขึ้นและประสิทธิภาพอยู่ในระดับมากที่สุด

4.5.4 ผลการวิจัยวัตถุประสงค์ข้อที่ 4 นำเสนอแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ใหม่ที่เหมาะสมกับองค์กร ภายใต้อาณัติความคิดที่ไม่ไว้วางใจใคร หากแต่ต้องตรวจสอบอยู่เสมอ ผลการวิจัยพบว่า การออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ใหม่ที่เหมาะสมกับองค์กร ซึ่งจากการประเมินการออกแบบนั้นมีความเหมาะสมและเห็นด้วยมากที่สุด นั้นต้องให้หลักความสำคัญอยู่ 5 ส่วนได้แก่ นโยบายความมั่นคงปลอดภัยสำหรับองค์กร เทคโนโลยีที่ใช้ในการป้องกันภัยคุกคามทางไซเบอร์สำหรับองค์กร การศึกษาและเรียนรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ การปรับเปลี่ยนการป้องกันอยู่เสมอให้ทันต่อปัจจุบัน การให้ความรู้แก่ทุกคนในองค์กรเพื่อป้องกันและรับภัยคุกคามทางไซเบอร์ หากกิจกรรมขององค์กร คลอบคลุมตามหลักการนี้ ก็สามารถให้องค์กรพร้อมรับเหตุการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ได้ในระดับมากที่สุด

บทที่ 5

สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

5.1 สรุปผลการวิจัย

การวิจัยครั้งนี้ ผลวิจัยแสดงให้เห็นการนำระบบ SIEM นำมาปรับใช้การป้องกันภัยคุกคามทางไซเบอร์ที่เกิดเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ การเข้าถึงจากภายนอกองค์กร และสามารถตอบสนองการป้องกันได้อยู่ในประสิทธิภาพในระดับมากที่สุด อีกทั้งสามารถนำไปปรับใช้งานในการป้องกัน ความแข็งแกร่ง ด้านการป้องกันภัยคุกคามทางไซเบอร์ให้มีประสิทธิภาพมากขึ้น นำไปดำเนินการเพื่อตอบวัตถุประสงค์ของการวิจัยตามลำดับ ดังต่อไปนี้

5.1.1 ผลการวิจัยตามวัตถุประสงค์ข้อที่ 1 เพื่อทำการวิเคราะห์ภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายในองค์กร ผลการวิจัยพบว่าระบบ SIEM สามารถทำการวิเคราะห์ และเปรียบเทียบค่าของ MITRE ATT&CK Framework เพื่อระบุภัยคุกคามที่เกิดขึ้นกับเครื่องแม่ข่ายที่เป็น Honeypot ได้มีประสิทธิภาพในระดับมาก โดยเหตุการณ์ที่เปรียบเทียบได้ 3 แบบ คือ

1. การค้นหาช่องทางบริการเครื่องแม่ข่าย หรือ Lateral Movement
2. การระบุการโจมตีเครื่องแม่ข่ายรูปแบบการสุ่มรหัสผ่าน หรือ Brute-Force SSH
3. การระบุถึงการเข้าเครื่องแม่ข่ายอย่างสมบูรณ์ หรือ Authentication Success

5.1.2 ผลการวิจัยตามวัตถุประสงค์ข้อที่ 2 พัฒนาระบบป้องกัน และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย โดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ ผลการวิจัยพบว่าการพัฒนาการป้องกัน และการแจ้งเตือน สามารถใช้ผลของการวิเคราะห์ข้อมูลที่เปรียบเทียบกับ MITRE ATT&CK Framework จากนั้นจะได้ค่าตัวถูกเงื่อนไขเพื่อใช้ในการกำหนดการตอบสนองเมื่อเกิดภัยคุกคามการโจมตีแบบ Brute-Force SSH โดยให้ระงับ หรือ Drop IP จากเครื่องต้นทางที่เข้ามาโจมตี และในขณะเดียวกันก็สามารถที่จะ แจ้งเตือนไปยังผู้ดูแลระบบให้สามารถทราบได้ว่ามีเกิดภัยคุกคามที่เครื่องคอมพิวเตอร์แม่ข่าย จากการนำเทคโนโลยีระบบ SIEM มาใช้จึงทำให้สามารถระบุภัยคุกคาม และแจ้งเตือนได้อย่างทันทั่วทั้งที่ อีกทั้งยังสามารถดำเนินการป้องกัน

หรือยับยั้งความเสียหายที่จะเกิดขึ้นกับเครื่องแม่ข่ายนั้น ไม่ให้เกิดขึ้นจากการเข้าถึงเครื่องแม่ข่ายจากผู้โจมตี

5.1.3 ผลการวิจัยตามวัตถุประสงค์ข้อที่ 3 เพื่อทำการประเมินประสิทธิภาพของระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย ผลการวิจัยพบว่าประสิทธิภาพการป้องกันเครื่องแม่ข่าย และการแจ้งเตือนมีความแม่นยำสูง ซึ่งการป้องกันมีประสิทธิภาพอยู่ในระดับมากที่สุด ($\bar{X}=5.00$) และ การแจ้งเตือนซึ่งมีประสิทธิภาพอยู่ในระดับมากที่สุด ($\bar{X}=5.00$) เช่นกัน

เมื่อระบบเกิดความพร้อมใช้ในการทดสอบ จึงได้นำระบบการป้องกันป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย โดยผู้ใช้งานจากหน่วยงานต่างๆ เช่น ภาครัฐ ภาคเอกชน และ ภาครัฐวิสาหกิจ จำนวน 68 ท่าน และเป็นภาคเอกชนจำนวน 60 ท่าน โดยมีค่าเฉลี่ย 4.34 และส่วนเบี่ยงเบนมาตรฐาน 0.64 ($\bar{X}=4.34$, S.D. = 0.64) ซึ่งความเหมาะสมและยอมรับอยู่ในระดับมากที่สุด และได้ผลการประเมินที่สูงกว่าสมมติฐานที่ตั้งไว้ในระดับมาก

5.1.4 ผลการวิจัยตามวัตถุประสงค์ข้อที่ 4 นำเสนอแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ใหม่ที่เหมาะสมกับองค์กร ภายใต้ฐานความคิดที่ไม่ไว้วางใจใคร หากแต่ต้องตรวจสอบอยู่เสมอ ผลการวิจัยพบว่าการพัฒนาระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ เมื่อหากพิจารณาแล้วกับหลักการ Zero Trust ซึ่งสามารถนำไปใช้ภายในองค์กรเพื่อการป้องกันภัยคุกคามทางไซเบอร์ และสามารถช่วยให้เครื่องแม่ข่ายขององค์กรมีความมั่นคงปลอดภัยมากขึ้น และนำเสนอการออกแบบ Proposed Zero Trust Security Architecture โดยจากการประเมินของผู้ทางคุณวุฒิ ซึ่งได้รับการประเมินความเหมาะสมและเห็นด้วยมากที่สุด รวมถึงการยอมรับก็อยู่ในระดับเหมาะสมมากที่สุด

5.2 อภิปรายผล

5.2.1 การใช้เทคนิคการวิเคราะห์ภัยคุกคามที่เกิดขึ้นกับเครื่องแม่ข่ายตามที่ได้กำหนดไว้ได้ ซึ่งจากการวิจัยผู้วิจัย ได้ทำการเก็บข้อมูล Log จากเครื่องแม่ข่ายเพื่อมาใช้ในการวิเคราะห์ข้อมูลจากการเปรียบเทียบกับข้อมูลของ MITRE ATT&CK หากเมื่อเกิดเหตุการณ์ภัยคุกคามกับเครื่องแม่ข่ายตรงตามค่าตัวแปรจากฐานข้อมูลของ MITRE ATT&CK ก็จะทำให้ทราบถึงภัยคุกคามที่จะเกิดขึ้นกับเครื่องแม่ข่ายได้อย่างถูกต้องและมีประสิทธิภาพในระดับมาก เพราะเทคนิคการโจมตีได้มีการตรวจเปรียบเทียบ

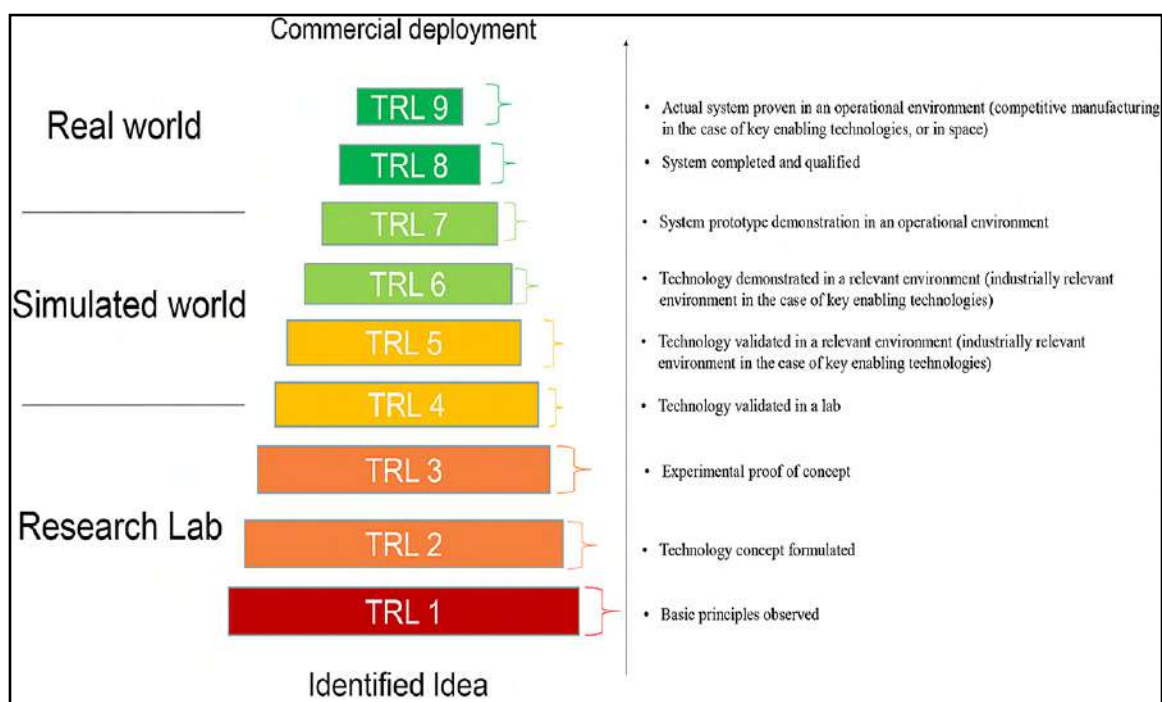
กำหนดการบันทึก ติดตั้งไว้ในระบบ SIEM เพื่อใช้เป็นเงื่อนไขการแจ้งเตือนไปยัง Slack ทำให้ผู้ดูแลทราบเหตุการณ์ได้โดยง่าย และยังสามารถส่งข้อมูลที่จำเป็นไปพร้อมการแจ้งเตือนภายในครั้งเดียวและลดระยะเวลาของการตรวจสอบเครื่องแม่ข่ายไปพร้อมกัน

5.2.2 การตอบสนองป้องกันและแจ้งเตือนเมื่อเกิดภัยคุกคามแบบเรียลไทม์ ผู้วิจัยได้ให้ความสำคัญเรื่องระยะเวลาการป้องกันเครื่องแม่ข่ายพร้อมกับแจ้งเตือนให้กับผู้ดูแลระบบ เพราะหากระบบ SIEM ยังสามารถแจ้งเหตุภัยคุกคามได้ใกล้เคียงกับระยะเวลาเกิดภัยคุกคามมากยิ่งขึ้น ก็จะยิ่งเพิ่มประสิทธิภาพในระดับมาก ต่อการป้องกันจากภัยคุกคามที่เกิดขึ้นกับเครื่องแม่ข่ายได้ดียิ่งขึ้น ซึ่งงานวิจัยสะท้อนผลการเปรียบเทียบระยะเวลาการป้องกัน และแจ้งเตือน พร้อมกับการบันทึกข้อมูลภัยคุกคามที่เกิดขึ้นนั้น มีค่าความต่างของเวลาไม่เกิน 10 วินาที นับจากเวลาเกิดเหตุภัยคุกคาม ก็ยังเป็นผลดีต่อการป้องกันภัยคุกคาม และสามารถนำระบบไปใช้งานจริงได้ ซึ่งความรวดเร็วในการประมวลผลนี้อาจจะต้องอาศัยประสิทธิภาพของระบบเครือข่ายหรืออินเทอร์เน็ตที่เชื่อมต่ออยู่ด้วยเพราะ จะเห็นได้ว่าการเตือนออกไปยัง Slack ที่ใช้งานอยู่นั้นจะต้องมีการส่งค่าการแจ้งเตือนออกไปผู้ให้บริการผ่านระบบอินเทอร์เน็ต แต่ยังสามารถใช้ได้โดยไม่มีค่าใช้จ่ายใดๆ ในการเรียกใช้ API ของ Slack และแจ้งไปยัง Application บน Mobile หรือ PC ซึ่งเป็นการเพิ่มความสะดวก และคล่องตัวให้กับผู้ดูแลระบบให้สามารถใช้งานได้ทุกที่ ที่อินเทอร์เน็ตสามารถใช้งานได้ และประหยัดค่าใช้จ่ายในการพัฒนา Application ที่ใช้ในการแจ้งเตือนอีกด้วย

5.2.3 การประเมิน Technology Readiness Level: TRL

การประเมิน Technology Readiness Level (TRL) หรือระดับความพร้อมทางเทคโนโลยี เป็นเครื่องมือที่ใช้ในการวัดและประเมินความก้าวหน้าของการพัฒนาเทคโนโลยีตั้งแต่แนวคิดเบื้องต้นไปจนถึงการนำไปใช้งานจริง TRL แบ่งออกเป็น 9 ระดับ โดยแต่ละระดับจะบ่งบอกถึงสถานะการพัฒนาเทคโนโลยีในขั้นตอนต่าง ๆ เช่น TRL 1 คือระดับที่แนวคิดพื้นฐานถูกสำรวจและพิสูจน์ในระดับทฤษฎี TRL 7 แสดงให้เห็นว่าเทคโนโลยีมีความเสถียรและความน่าเชื่อถือในระดับที่สูงขึ้นจากการทดสอบในห้องปฏิบัติการ (TRL 4-6) และสามารถดำเนินการได้ในสภาพแวดล้อมที่ซับซ้อนมากขึ้นที่ใกล้เคียงกับการใช้งานจริง สุดท้าย TRL 9 คือระดับที่เทคโนโลยีได้ถูกนำไปใช้งานจริงในสภาพแวดล้อมที่ตั้งใจ ทั้งนี้เพื่อให้ผู้ที่เกี่ยวข้องสามารถประเมินความเสี่ยงและความเป็นไปได้ของการนำเทคโนโลยีไปใช้ในขั้นตอนต่าง ๆ ได้อย่างมีประสิทธิภาพ

จากการวิจัยครั้งนี้ พบว่าผลที่ได้จากการวิจัยนี้อยู่ในระดับอยู่ในระดับ TRL 7 หรือ Final development version of the deliverable demonstrated in operational เป็นการทดสอบในสภาวะจริง โดยเปิดให้สามารถเข้าถึงจากเครือข่ายสาธารณะได้ และทดสอบจากเครื่องคอมพิวเตอร์แม่ข่าย ที่เป็น Honeypot ซึ่งผลของการทดสอบสามารถนำไปใช้เป็นต้นแบบ ที่ผ่านการพิสูจน์จากการใช้งานจริง ณ สภาวะการทำงานจริง และทำงานบนระบบคลาวด์ จริงๆ ดังภาพประกอบที่ 5.1



ภาพประกอบที่ 5.1 ระดับความพร้อมของความรู้และเทคโนโลยีทางด้านเทคโนโลยี

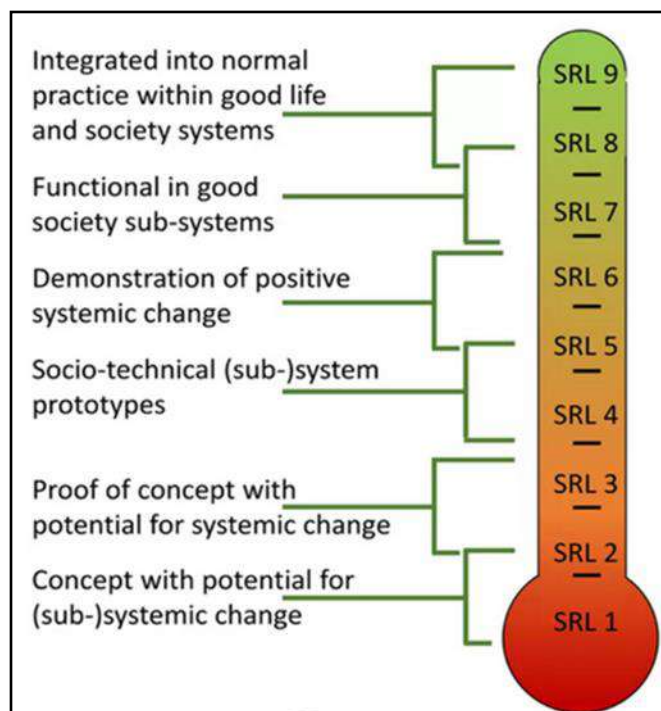
ที่มา : frontiersin.org, 2022

5.2.4 การประเมิน Societal Readiness Level: SRL

การประเมิน Societal Readiness Level (SRL) หรือระดับความพร้อมทางสังคม เป็นเครื่องมือที่ใช้ในการวัดและประเมินความพร้อมของเทคโนโลยีหรือโครงการในด้านการยอมรับและผลกระทบ ต่อสังคม SRL ช่วยให้ผู้พัฒนาเทคโนโลยี นักวิจัย และผู้จัดการโครงการสามารถประเมินว่าผลิตภัณฑ์ หรือโครงการนั้น ๆ มีความพร้อมในการถูกรับรู้และยอมรับจากผู้ใช้งานและสังคมโดยรวมได้มากน้อย

เพียงใด การประเมิน SRL มุ่งเน้นไปที่การพิจารณาปัจจัยทางสังคม วัฒนธรรม จริยธรรม กฎหมาย และความยั่งยืน ที่อาจส่งผลต่อการนำเทคโนโลยีหรือโครงการมาใช้งานจริง เช่น SRL 1-3 เป็นระดับแนวคิดและการศึกษาเบื้องต้น SRL 4-6 เป็นระดับการทดสอบและการประเมินผลกระทบทางสังคม และ SRL 7-9 เป็นระดับการนำไปใช้งานจริงและการยอมรับในวงกว้าง

จากการวิจัยครั้งนี้ พบว่าผลที่ได้จากการวิจัยนี้อยู่ใน SRL 6 หรือ Demonstration of Positive Systemic Change เป็นการทดลองเทคโนโลยีหรือโครงการในสภาพแวดล้อมที่ใกล้เคียงกับการใช้งานจริง พร้อมกับการประเมินผลกระทบทางสังคมในวงกว้าง และสามารถนำไปปรับใช้ หรือประยุกต์กับสิ่งแวดล้อมหรือเงื่อนไขอื่นๆ โดยสามารถดำเนินการกับผู้ใช้งานในสภาพแวดล้อมด้านอื่นๆ เพื่อให้ได้ข้อเสนอแนะผลทดสอบเบื้องต้นที่เป็นไปได้ดังภาพประกอบที่ 5.2



ภาพประกอบที่ 5.2 ระดับความพร้อมของความรู้และเทคโนโลยีทางด้านสังคม

ที่มา : Lancaster University, 2020

งานวิจัยของผู้วิจัยฉบับนี้ ได้มุ่งมองการใช้ระบบป้องกันภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย ด้วยการทำงานวิเคราะห์เหตุการณ์ตามเงื่อนไขที่กำหนด ซึ่งมีความมุ่งหวังไปยังภาคเอกชนกลุ่มวิสาหกิจขนาดกลางและขนาดย่อม หรือ SME หรือหน่วยงานอื่นๆ เพื่อโดยการวิจัยนี้สามารถนำไปใช้ประโยชน์ โดยสรุปแบบรวม ได้ดังนี้

ในแง่ของผลผลิต (Outputs) ของงานวิจัยฉบับนี้ คือ

การพัฒนา ระบบ SIEM เพื่อใช้ในการป้องกันและแจ้งเตือนการโจมตีทางไซเบอร์แบบเรียลไทม์ ทำให้สามารถป้องกันการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายจากการเรียนรู้ Log System ที่เกิดขึ้นและนำมาวิเคราะห์ตามเงื่อนไขที่กำหนดได้อย่างมีประสิทธิภาพระดับดีมาก

ในแง่ของผลลัพธ์ (Outcomes) ของงานวิจัยฉบับนี้ คือ

แนวทางการนำไปพัฒนาใช้งานภายในองค์กรที่ต้องการป้องกัน และเสริมสร้างความมั่นคงปลอดภัยเครื่องคอมพิวเตอร์แม่ข่ายทางไซเบอร์ แบบไม่มีค่าใช้จ่ายที่ต่ำกว่า การใช้แบบมี License และสามารถปรับปรุงแก้ไขขอบเขตการป้องกันให้มีวงกว้างและมีประสิทธิภาพมากขึ้น

ในแง่ของผลกระทบ (Impacts) ของงานวิจัยฉบับนี้ คือ

สามารถนำผลผลิตจากการพัฒนามาสร้างระบบป้องกันเครื่องคอมพิวเตอร์แม่ข่ายจากการวิเคราะห์เหตุการณ์ที่บันทึกขึ้น จึงสามารถเรียนรู้พฤติกรรมของผู้โจมตี ว่ามีกระบวนการหรือแนวทางอย่างไร ในการเข้าโจมตีหรือความพยายามเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

อย่างไรก็ตาม เมื่อกล่าวโดยสรุปถึงประโยชน์ในด้านต่าง ๆ ของงานวิจัยฉบับนี้ มีดังนี้ คือ

ประโยชน์ด้านวิชาการ

1. พัฒนาความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นการวิจัยนี้ช่วยเพิ่มความรู้และความเข้าใจเกี่ยวกับการใช้สถาปัตยกรรม Zero Trust ในการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะในสภาพแวดล้อมที่ต้องการความมั่นคงปลอดภัยสูงสุด
2. เป็นแนวทางการพัฒนาสถาปัตยกรรมใหม่ สามารถใช้เป็นกรณีศึกษาและแนวทางสำหรับนักวิจัยหรือผู้ที่สนใจในการพัฒนาสถาปัตยกรรมความมั่นคงปลอดภัยใหม่ ๆ ในอนาคต

3. ส่งเสริมการศึกษาและการเรียนรู้ผลการวิจัยนี้สามารถนำไปใช้เป็นเนื้อหาสำหรับการเรียนการสอนในระดับมหาวิทยาลัย หรือสถาบันการศึกษาที่มีการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์

ประโยชน์ด้านเศรษฐกิจ

1. ลดความเสี่ยงทางการเงินจากการโจมตีทางไซเบอร์ การนำสถาปัตยกรรม Zero Trust มาใช้สามารถช่วยลดความเสี่ยงจากการโจมตีทางไซเบอร์ที่อาจก่อให้เกิดความเสียหายทางการเงินต่อองค์กร
2. เพิ่มประสิทธิภาพและลดค่าใช้จ่ายในการบริหารจัดการความมั่นคงปลอดภัยการมีระบบที่สามารถตรวจสอบและป้องกันภัยคุกคามได้อย่างมีประสิทธิภาพจะช่วยลดค่าใช้จ่ายที่เกี่ยวข้องกับการจัดการเหตุการณ์ทางไซเบอร์และการฟื้นฟูระบบ
3. ส่งเสริมความเชื่อมั่นและสร้างมูลค่าให้แก่องค์กรการมีระบบความมั่นคงปลอดภัยที่เชื่อถือได้จะสร้างความเชื่อมั่นให้กับลูกค้าและผู้มีส่วนได้ส่วนเสีย ซึ่งสามารถสร้างมูลค่าและความยั่งยืนให้แก่องค์กรในระยะยาว

ประโยชน์ด้านสังคม

1. เพิ่มความตระหนักรู้และความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในสังคมการวิจัยนี้ช่วยเพิ่มความตระหนักรู้เกี่ยวกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์ในระดับสังคม ทำให้ประชาชนทั่วไปมีความรู้และระมัดระวังมากขึ้น
2. ส่งเสริมการใช้งานเทคโนโลยีอย่างปลอดภัย ช่วยสร้างแนวทางและมาตรฐานการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย ซึ่งจะส่งผลให้การใช้งานอินเทอร์เน็ตและระบบคอมพิวเตอร์ในสังคมมีความมั่นคงปลอดภัยมากขึ้น รวมทั้งประยุกต์ใช้ในหน่วยงานต่าง ๆ เช่น วิสาหกิจขนาดกลางและขนาดย่อมหรือ SMEs ในประเทศไทย
3. ลดการเกิดอาชญากรรมทางไซเบอร์ด้วยการนำเสนอวิธีการและมาตรการป้องกันที่มีประสิทธิภาพ สามารถช่วยลดจำนวนเหตุการณ์อาชญากรรมทางไซเบอร์ ซึ่งจะส่งผลดีต่อความมั่นคงปลอดภัย

ประโยชน์ด้านนโยบาย

1. การนำสถาปัตยกรรม Zero Trust Security มาใช้ในองค์กรนั้นเป็นนโยบายที่สำคัญในการเพิ่มประสิทธิภาพในการป้องกันภัยคุกคามทางไซเบอร์ สถาปัตยกรรมใหม่นี้ถูกพัฒนาขึ้นเพื่อปรับปรุง

ระดับความพร้อมทางไซเบอร์และการรับมือกับความเล็งและภัยคุกคามทางไซเบอร์ ซึ่งได้รับการยอมรับและเห็นด้วยในระดับสูงสุดจากผู้เชี่ยวชาญที่เข้าร่วมการประเมิน

2. การใช้ Framework และ Standard เช่น NIST Framework 2.0, Zero Trust Framework, Security Mesh Framework และอื่นๆ ช่วยในการจัดการและลดความเสี่ยงทางไซเบอร์ในองค์กรได้อย่างมีประสิทธิภาพ นโยบายนี้ช่วยให้การป้องกันและการตอบสนองต่อเหตุการณ์เป็นไปอย่างรวดเร็วและมีประสิทธิภาพมากขึ้น โดยเฉพาะในส่วนของ การควบคุมการเข้าถึง และการกักกันข้อมูลที่มีประสิทธิภาพ

3. นโยบายการนำ Framework และ Standard ด้านความมั่นคงปลอดภัยทางไซเบอร์เข้ามาใช้ เพื่อเพิ่มความมั่นคงปลอดภัย แต่ยังสนับสนุนการดำเนินธุรกิจขององค์กรให้มีประสิทธิภาพมากขึ้น โดยการทำให้การป้องกันภัยคุกคามเป็นไปอย่างรวดเร็วและลดความซับซ้อนในการจัดการระบบข้อมูล นอกจากนี้ยังส่งเสริมให้มีการตรวจสอบและปรับปรุงระบบความมั่นคงปลอดภัยอย่างต่อเนื่อง ซึ่งเป็นปัจจัยสำคัญในการรักษามาตรฐานและความมั่นคงของข้อมูลในองค์กร

5.3 ปัญหาและอุปสรรคในการทำวิจัย

การวิจัยในเรื่องที่ศึกษานี้ ระหว่างดำเนินการได้พบกับปัญหา และอุปสรรค ตามขั้นตอนต่าง ๆ ซึ่งสิ่งเหล่านั้นส่งผลต่อระยะเวลา รูปแบบ ขั้นตอน ค่าใช้จ่าย ที่เกี่ยวกับการวิจัยดังนี้

5.3.1 การรวบรวมข้อมูล

ในการรวบรวมข้อมูลต้องใช้เวลาในการรวบรวมอย่างน้อย 14 วันขึ้นไปเพื่อดูเหตุการณ์ หรือ พฤติกรรมการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายที่เกิดขึ้นอย่างสม่ำเสมอ และต่อเนื่องเพื่อใช้ในการประเมินและทดสอบเงื่อนไขที่กำหนดไว้ในระบบ SIEM หากใช้ข้อมูลที่น้อยกว่านี้อาจจะไม่สามารถเห็น เหตุการณ์อื่นๆ ที่อาจจะมีแตกต่างออกไปจากการวิเคราะห์ และดูการตอบสนองการป้องกันได้อย่างถูกต้อง

5.3.2 การแก้ไขชุดคำสั่งการอ่านข้อมูล

การแก้ไขชุดคำสั่งที่ให้อ่านข้อมูลเพื่อเปรียบเทียบกับที่ตั้งไว้ในระบบ SIEM ต้องมีความถูกต้องอย่างมาก หากไม่ถูกต้องก็อาจจะไม่ทำการเปรียบเทียบ และไม่ตอบสนองชุดคำสั่งที่ได้มีการกำหนดไว้ และส่งผลต่อการป้องกันเครื่องแม่ข่ายก็ไม่ทำงานตามไปด้วย จึงเป็นสิ่งต้องพึงระวังในการแก้ไขชุดคำสั่งหรือมีการทดสอบหลายๆ ครั้งจนกว่าแน่ใจว่าสมบรณ์ จึงนำไปปรับใช้กับในระบบ SIEM

5.4 ข้อเสนอแนะ

การศึกษาวิจัย การพัฒนาระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ ผู้วิจัยมีจึงข้อเสนอแนะจากการศึกษาค้างนี้ดังนี้

5.4.1 ข้อเสนอแนะสำหรับการนำผลวิจัยไปใช้งาน

1. การปรับใช้ระบบ SIEM

ควรนำระบบ SIEM ที่ได้จากการวิจัยนี้ไปปรับใช้ในองค์กร เพื่อเพิ่มความแข็งแกร่งในการป้องกันภัยคุกคามทางไซเบอร์และเพิ่มประสิทธิภาพในการวิเคราะห์เหตุการณ์ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่าย

2. การแจ้งเตือนผ่านแอปพลิเคชัน Slack

นำระบบการแจ้งเตือนภัยคุกคามทางไซเบอร์แบบเรียลไทม์ที่พัฒนาขึ้นไปใช้งาน โดยเฉพาะการแจ้งเตือนผ่านแอปพลิเคชัน Slack ซึ่งช่วยให้ผู้ดูแลระบบสามารถตอบสนองต่อเหตุการณ์โจมตีได้ทันที

3. การวิเคราะห์จุดอ่อนและเสริมความมั่นคงปลอดภัย

ใช้ผลการวิจัยในการวิเคราะห์จุดอ่อนของระบบเครื่องคอมพิวเตอร์แม่ข่ายและปรับปรุงมาตรการความมั่นคงปลอดภัย เพื่อป้องกันการโจมตีในอนาคตและลดความเสี่ยงที่อาจเกิดขึ้น

5.4.2 ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

1. การพัฒนาและปรับปรุงเทคโนโลยีการป้องกัน

ควรทำการวิจัยเพิ่มเติมเพื่อพัฒนาเทคโนโลยีการป้องกันภัยคุกคามทางไซเบอร์ให้มีประสิทธิภาพมากยิ่งขึ้น โดยเน้นที่การตรวจจับและตอบสนองต่อภัยคุกคามในเวลาจริงได้ดียิ่งขึ้น

2. การวิเคราะห์และประเมินผลการใช้ระบบในสภาพแวดล้อมจริง

ทำการวิจัยเพื่อประเมินผลการใช้ระบบป้องกันภัยคุกคามในสภาพแวดล้อมจริง เพื่อให้ได้ข้อมูลที่ถูกต้องและสามารถปรับปรุงระบบให้เหมาะสมกับการใช้งานในสถานการณ์จริงได้ดียิ่งขึ้น

3. การศึกษาเพิ่มเติมในเทคนิคการวิเคราะห์เหตุการณ์

วิจัยเพิ่มเติมเกี่ยวกับเทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคาม เพื่อหาแนวทางใหม่ๆ ที่สามารถนำมาใช้ในการพัฒนาระบบป้องกันภัยคุกคามได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

5.4.3 ข้อเสนอแนะเชิงนโยบาย

1. นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับองค์กร

ควรมีการกำหนดนโยบายความมั่นคงปลอดภัยไซเบอร์ที่ชัดเจนและครอบคลุม โดยนำหลักการ Zero Trust มาใช้ ซึ่งหมายถึงการไม่ไว้ใจใครและต้องตรวจสอบเสมอ เพื่อให้มั่นใจว่าข้อมูลและระบบขององค์กรมีความมั่นคงปลอดภัยจากภัยคุกคามไซเบอร์

2. การบังคับใช้นโยบายการฝึกอบรมและการรับรู้ด้านความมั่นคงปลอดภัยไซเบอร์

องค์กรควรมีการฝึกอบรมและเสริมสร้างความรู้ความเข้าใจด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่พนักงานทุกระดับอย่างต่อเนื่อง เพื่อให้ทุกคนสามารถปฏิบัติตามนโยบายและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยได้อย่างถูกต้อง

3. นโยบายการลงทุนในเทคโนโลยีและเครื่องมือด้านความมั่นคงปลอดภัยไซเบอร์

ควรมีการลงทุนในเทคโนโลยีและเครื่องมือที่ทันสมัยสำหรับการตรวจสอบและป้องกันภัยคุกคามไซเบอร์ เช่น ระบบ SIEM (Security Information and Event Management) ซึ่งสามารถช่วยในการรวบรวม วิเคราะห์ และตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ

ผู้วิจัยหวังว่า ข้อเสนอแนะเบื้องต้นดังกล่าวมานั้นจะมีประโยชน์ไม่มากนักสำหรับผู้ที่จะนำไปศึกษาวิจัยต่อไป และสามารถนำการออกแบบ Proposed Zero Trust Security Architecture ไปปรับใช้จริง เพื่อศึกษาต่อถึงการทำงานและการเปลี่ยนผ่านจากการออกแบบเดิมไปสู่การออกแบบ Zero Trust Security Architecture อีกด้วย หากจะเป็นพระคุณอย่างยิ่งถ้างานวิจัยนี้มีผู้ที่นำไปทำประโยชน์ หรือวิจัยขยายผลเพื่อประโยชน์เป็นส่วนรวมสำหรับอนาคตข้างหน้า

บรรณานุกรม

- กรกัญญ์ณารักษ์ บุญสุขเกิด. (2564). สถานการณ์และแนวทางการป้องกันอาชญากรรมไซเบอร์ในประเทศไทย. *RPCA Journal of Criminology and Social Sciences*, 3(1), 33-47.
- กิตติ ประเสริฐสุข. (2562). ไทยกับความมั่นคงรูปแบบใหม่: การค้ามนุษย์ การย้ายถิ่นแบบไม่ปกติ อาชญากรรมข้ามชาติ และความมั่นคงปลอดภัยไซเบอร์. สถาบันเอเชียตะวันออกเฉียงใต้ศึกษา มหาวิทยาลัยธรรมศาสตร์.
- กิตติคุณ พละการ กิตติภพ พละการ สมชาย ประสิทธิ์จูตระกูล และสุกรี สินธุภิญโญ. (2561). Python ๑๐๑. พิมพ์ครั้งที่ 2. คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.
- คริสณะ ฉิมมณี. (2564). แนวทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ในเขตพื้นที่พุทธสถานกรณีศึกษาเมสแก้ง. วิทยาลัยนวัตกรรมการผลิตเทคโนโลยี มหาวิทยาลัยรังสิต.
- ชรินทร์ทิพย์ ปันสุวรรณ. (2565). แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล. คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.
- ณิชาธิ์ ลิมปนเทวินทร์. (2562). ปัจจัยพยากรณ์ด้านพฤติกรรมการใช้งานสื่อสังคมออนไลน์ ด้านพฤติกรรมความเสี่ยงต่อการโดนโจรกรรมข้อมูลและด้านความรู้เท่าทันสื่อกับความปลอดภัยบนโลกไซเบอร์ของกลุ่ม Generation Y, 37-54. วารสารนิเทศศาสตร์และนวัตกรรม ปีที่ 6 ฉบับที่ 1.
- ฐกฤต แก้วทับทิม. (2564). การขยายตัวขององค์กรอาชญากรรมไซเบอร์ในช่วงการระบาดของโควิด-19. วารสารวิชาการอาชญาวิทยาและนิติวิทยาศาสตร์ มหาวิทยาลัยมหิดล.
- ธนพงศ์ ฉันทวิเชียร. (2566). การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9. มหาวิทยาลัยสงขลานครินทร์.
- ธรัช พงษ์ชนี. (2562). ระบบเฝ้าระวังและตรวจจับภัยคุกคามเว็บเซิร์ฟเวอร์ Mini SOC Web Server. คณะวิทยาการและเทคโนโลยีสารสนเทศ. มหาวิทยาลัยเทคโนโลยีมหานคร.
- นิลमित นิลาส. (2560). การศึกษากระบวนการทำงานของ Mirai Botnet ในความปลอดภัยด้านไซเบอร์ของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร. คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร.
- นริศ อุไรพันธ์. (2565). ปัจจัยที่ส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของธุรกิจพาณิชย์

- อิเล็กทรอนิกส์ สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย. URU-J. ISSN 2821-9708, 12(1), 1-19.
- ปรเมศวร์ กุมาบุญ. (2563). ความสัมพันธ์ระหว่างการใช้ตัวตนกับอาชญากรรมไซเบอร์. คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์. (2564). ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ.
- ภัทร ลีลาพทุธิ์. (2565). การเขียนโปรแกรมภาษาไพทอนด้วยการเรียนรู้ด้วยตนเอง. ภาควิชาวิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์.
- วิไล ฤทธิเดช. (2565). ความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ ของบุคลากรสาธารณสุขในประเทศไทย: กรณีศึกษาโรงพยาบาลพุทธโสธร. บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร.
- สุรพงศ์ ทรัพย์าคม. (2563). การวิเคราะห์การรักษาความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. งานประชุมวิชาการระดับชาติ มหาวิทยาลัยรังสิต ประจำปี 2563.
- สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2566). Zero Trust Model เกราะคุ้มกันจากภัยคุกคามไซเบอร์.
- สำนักงานราชบัณฑิตยสภา. (2562). ราชบัณฑิตยสถานคอมพิวเตอร์และเทคโนโลยีสารสนเทศ. [ออนไลน์]. เข้าถึงได้จาก <https://th-th.facebook.com/RatchabanditThai>. วันที่สืบค้น 15 ตุลาคม 2566.
- สุบิน ชุระรัช. (2565) ทำไมต้องลิเคิร์ต?. วารสารนวัตกรรมและการจัดการ ศูนย์ส่งเสริมและพัฒนางานวิจัย มหาวิทยาลัยศรีปทุม.
- อเนชพันธ์ นิธินันท์นฤมิต. (2563). การเสริมสร้างทักษะการเผชิญปัญหาการถูกกลั่นแกล้งทางไซเบอร์ของนักเรียนโดยการให้คำปรึกษากลุ่มแบบบูรณาการ. บัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ.
- เอกชัย พ่วงพรพิทักษ์ และคณะ (2565). การพัฒนาแนวทางการสืบสวนอาชญากรรมทางไซเบอร์ต่อบริการธนาคารอิเล็กทรอนิกส์ และวิเคราะห์เทคนิคเทคโนโลยีสารสนเทศ. กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม.
- Baker, D. J. (2018). The concept of cybercrime: Applying the general part to limit offending via cyber means. University of Cambridge.

- Bendovschi, A. (2015). Cyber attacks Trends, patterns and security countermeasures. *Procedia Economics and Finance*, 28, 24-31.
- Buresh, D. L. (2022, May 25). A Practical Evaluation of Remote Work Issues and the SolarWinds Breach Using the ISO/IEC 27001 Cybersecurity Framework and the ISO/IEC 27002 Guidelines. *Studies in Social Science Research*.
- Cisco. (2021). Cybersecurity for SMBs Asia Pacific businesses prepare for digital defense. [ออนไลน์]. เข้าถึงได้จาก https://www.cisco.com/c/en_sg/products/security/cybersecurity-for-smbs-in-asia-pacific/index.html. วันที่สืบค้น 20 ตุลาคม 2566.
- CISA. (2023). Zero trust maturity model. Version 2.0. Cybersecurity and Infrastructure Security Agency.
- Cyfence. (2022). SIEM หัวใจของการตรวจจับภัยคุกคามไซเบอร์. [ออนไลน์]. เข้าถึงได้จาก <https://www.cyfence.com/article/what-is-siem>. วันที่สืบค้น 15 ตุลาคม 2566.
- Divya P., & Sherin, S. (2022). A zero trust framework security to prevent data breaches and mitigate the cloud network attacks. *International Journal for Research in Applied Science and Engineering Technology*, 10(5), 3530-3538.
- Elliott, G. (2004). *Global business information technology An integrated systems approach*.
- Etzioni, A. (2014). A cyber age privacy doctrine: A liberal communitarian approach. *A Journal of Law and Policy for Information Society*.
- Filkins, B. (2019). *An evaluator's guide to NextGen SIEM*. SANS Institute.
- Fortinet. (2023). What is a brute force attack. [ออนไลน์]. เข้าถึงได้จาก <https://www.fortinet.com/resources/cyberglossary/brute-force-attack>. วันที่สืบค้น 15 ตุลาคม 2566.
- Stefanini IT Solution. (2021). What is cybersecurity mesh? 5 advantages of this top technology trend. [ออนไลน์]. เข้าถึงได้จาก <https://stefanini.com/en/insights/news/what-is-cybersecurity-mesh-5-advantages-of-this-top-tech-trend>. วันที่สืบค้น 15 ตุลาคม 2566.
- HUNTSMAN. (2018). *The essential guide to SIEM next generation security monitoring*. Tier-3 Pty Ltd.
- IBM. (2023). What is SIEM. [ออนไลน์]. เข้าถึงได้จาก <https://www.ibm.com/topics/siem>. วันที่สืบค้น 15 ตุลาคม 2566.
- Kasetsart University. (2022). กฎของมัวร์ (Moore's law). [ออนไลน์]. เข้าถึงได้จาก https://web.ku.ac.th/schoolnet/snet7/moore_1.htm. วันที่สืบค้น 15 ตุลาคม 2566.

- Karel, H., Tomas, B., Tomas, C., & Hana, K. (2021). Refined detection of SSH brute-force attackers using machine learning. HAL Open Science.
- Lumb, D. (2014). This story about Slack's founder says everything you need to know about him. [ออนไลน์]. เข้าถึงได้จาก <https://www.fastcompany.com/302641him.his-story-about-slacks-founder-says-everything>. วันที่สืบค้น 15 ตุลาคม 2566.
- Machado, H. (2021). Zero trust security model - How does it affect IT security management. [ออนไลน์]. เข้าถึงได้จาก <https://www.linkedin.com/pulse/zero-trust-security-model-how-does-affect-hiram-machado>. วันที่สืบค้น 15 ตุลาคม 2566.
- Maghfirah, F., & Husna, F. (2022). Cybercrime and privacy right violation cases of online loans in Indonesia. Proceedings: Dirundeng International Conference on Islamic Studies.
- Malviya, V., & Aslekar, A. (2022). Cyber laws and modern surveillance; public protection or privacy violation. DOI:10.13140/RG.2.2.14437.45288.
- McCaughey, M., & Cermele, J. (2021). Violations of sexual and information privacy understanding dataraid in a (cyber)rape culture. Appalachian State University.
- Mingyang, X., Haoyu, Y., & Xinyue, Y. (2023). Zero-trust security authentication based on SPA endogenous security architecture. Electronics.
- Mohana, P., & Abhijit, R. (2022). Cyber awareness learning imitation environment (CALIE): A card game to provide cyber security awareness for various groups of practitioners. Int. J. Advanced Networking and Applications, 14.
- Muhammad, S., Muhammad, A., Mansoor, U., & Muhammad, H. (2023). Effective security monitoring using efficient SIEM architecture. Human-centric Computing and Information Sciences.
- NCSC-TG-004. (1988). Glossary of computer security terms. [ออนไลน์]. เข้าถึงได้จาก <https://irp.fas.org/nsa/rainbow/tg004.htm>. วันที่สืบค้น 15 ตุลาคม 2566.
- Nurse, J. R. C. (2021). Cybersecurity awareness. Encyclopedia of Cryptography, Security and Privacy.
- Park, J., Kim, J., Gupta, B., & Park, N. (2021). Network log-based SSH brute-force attack detection model. Computers, Materials & Continua, 887-901.

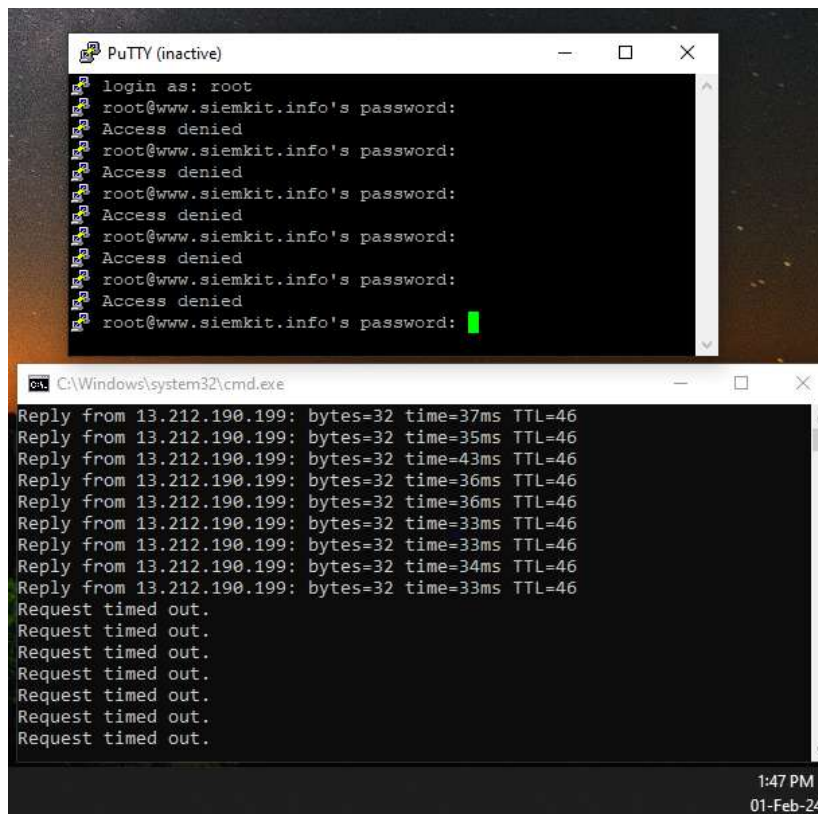
- Piyawan, C. (2021). เมื่อข้อมูลถูกโจรกรรม สำรวจ Cyber Attack ช่วง COVID-19 ธุรกิจไหนตกเป็นเป้าหมายที่สุด. [ออนไลน์]. เข้าถึงได้จาก <https://thematter.co/social/cyber-attack-in-covid-19/143794>. วันที่สืบค้น 15 ตุลาคม 2566.
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. NIST Special Publication, 800-207.
- Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. IEEE Access, 10, 57143-57179.
- Vlad-Mihai, C. (2015). SIEM (security information and event management solutions) implementation in private or public clouds. Scientific Bulletin of Naval Academy.
- Zhang, S., Xie, X., & Xu, Y. (2020). A brute-force black-box method to attack machine learning-based systems in cybersecurity. IEEE Access, 8, 128250-128263.
- Zanzig, J. S. (2022). Using the NIST Framework and COBIT 2019 in Offering Cybersecurity Consulting and Assurance Services. ใน IGI Global eBooks (หน้า 101-124). Jacksonville State University.

ภาคผนวก ก

แบบทดสอบประสิทธิภาพการวิเคราะห์การป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องแม่ข่ายคอมพิวเตอร์โดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองแบบเรียลไทม์

1. การทดสอบตามเงื่อนไขที่100030

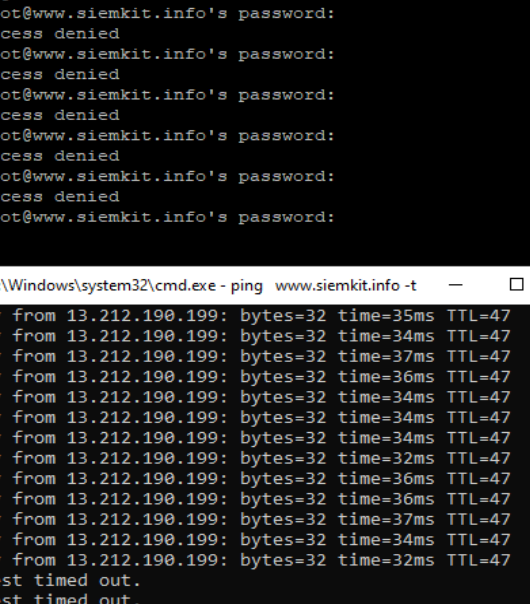
1.1 ทดสอบการวิเคราะห์และป้องกันบนเครื่องแม่ข่ายแบบเรียลไทม์



ภาพประกอบที่ ก.1 เงื่อนไขที่100030ทดสอบครั้งที่ 1

[illegible]

ภาพประกอบที่ ก.4 เงื่อนไขที่100030ทดสอบครั้งที่ 4



The image displays two terminal windows. The top window is a PuTTY session connected to www.siemkit.info, showing a root user attempting to log in with a password. The bottom window is a Windows command prompt running a ping command to the same IP address.

Terminal 1 (PuTTY):

```
www.siemkit.info - PuTTY
login as: root
root@www.siemkit.info's password:
Access denied
root@www.siemkit.info's password:
Access denied
root@www.siemkit.info's password:
Access denied
root@www.siemkit.info's password:
Access denied
root@www.siemkit.info's password:
Access denied
root@www.siemkit.info's password:
Access denied
root@www.siemkit.info's password:
```

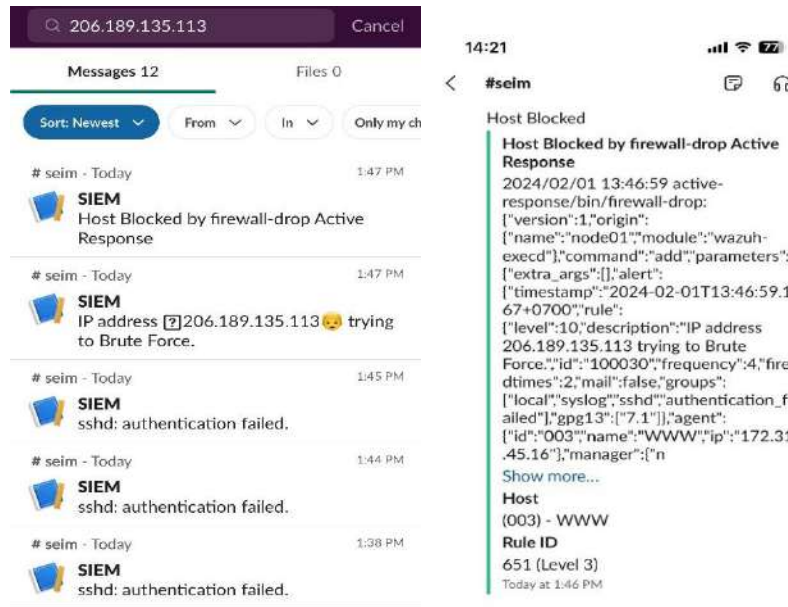
Terminal 2 (Windows Command Prompt):

```
C:\Windows\system32\cmd.exe - ping www.siemkit.info -t
Reply from 13.212.190.199: bytes=32 time=35ms TTL=47
Reply from 13.212.190.199: bytes=32 time=34ms TTL=47
Reply from 13.212.190.199: bytes=32 time=37ms TTL=47
Reply from 13.212.190.199: bytes=32 time=36ms TTL=47
Reply from 13.212.190.199: bytes=32 time=34ms TTL=47
Reply from 13.212.190.199: bytes=32 time=34ms TTL=47
Reply from 13.212.190.199: bytes=32 time=34ms TTL=47
Reply from 13.212.190.199: bytes=32 time=32ms TTL=47
Reply from 13.212.190.199: bytes=32 time=36ms TTL=47
Reply from 13.212.190.199: bytes=32 time=36ms TTL=47
Reply from 13.212.190.199: bytes=32 time=37ms TTL=47
Reply from 13.212.190.199: bytes=32 time=34ms TTL=47
Reply from 13.212.190.199: bytes=32 time=32ms TTL=47
Request timed out.
Request timed out.
```

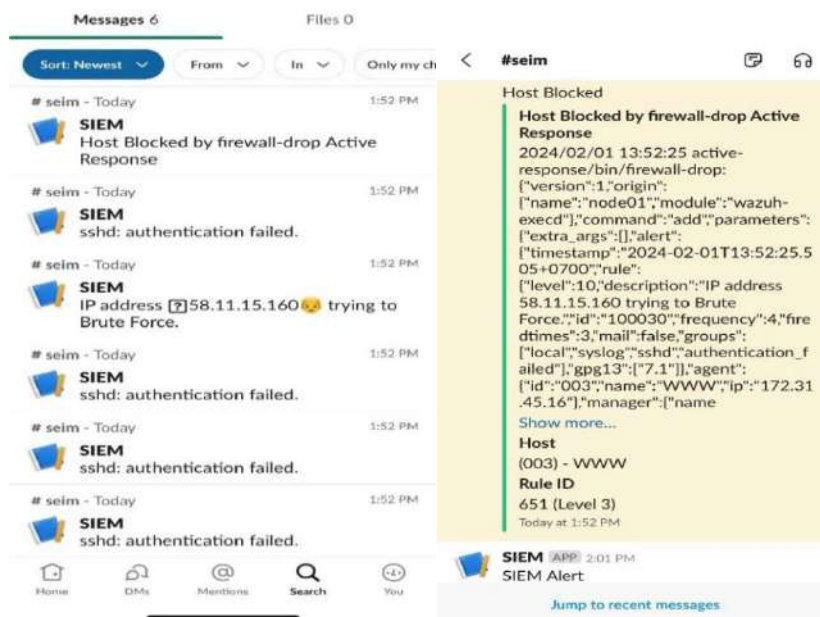
System Clock: 3:40 PM, 01-Feb-24

ภาพประกอบที่ ก.5 เงื่อนไขที่ 100030ทดสอบครั้งที่ 5

1.2 ทดสอบการวิเคราะห์และแจ้งเตือนภัยคุกคามบนเครื่องแม่ข่ายแบบเรียลไทม์



ภาพประกอบที่ ก.6 แจ้งเตือน100030ทดสอบครั้งที่ 1



ภาพประกอบที่ ก.7 แจ้งเตือน100030ทดสอบครั้งที่ 2

Messages 12 Files 0

Sort: Newest From In Only my ch

seim - Today 2:35 PM

SIEM
Host Blocked by firewall-drop Active Response

seim - Today 2:35 PM

SIEM
sshd: authentication failed.

seim - Today 2:35 PM

SIEM
IP address 58.11.15.160 trying to Brute Force.

seim - Today 2:35 PM

SIEM
sshd: authentication failed.

seim - Today 2:35 PM

SIEM
sshd: authentication failed.

seim - Today 2:35 PM

SIEM
sshd: authentication failed.

SIEM APP
Today at 2:35 PM

Host Blocked

Host Blocked by firewall-drop Active Response

2024/02/01 14:35:37 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"node01","module":"wazuh-execd"},"command":"add","parameters":{"extra_args":"","alert":{"timestamp":"2024-02-01T14:35:37.531+0700","rule":{"level":10,"description":"IP address 58.11.15.160 trying to Brute Force","id":"100030","frequency":4,"firedtimes":1,"mail":false,"groups":["local","syslog","sshd","authentication_failed"],"pgp13":["7.1"]},"agent":{"id":"003","name":"WWW","ip":"172.31.45.16"},"manager":{"name

Show more...

Host
(003) - WWW

Rule ID
651 (Level 3)
Today at 2:35 PM

ภาพประกอบที่ ก.8 แจ้งเตือน100030ทดสอบครั้งที่ 3

Messages 17 Files 0

Sort: Newest From In Only my ch

seim - Today 2:51 PM

SIEM
Host Blocked by firewall-drop Active Response

seim - Today 2:51 PM

SIEM
IP address 58.11.15.160 trying to Brute Force.

seim - Today 2:51 PM

SIEM
sshd: authentication failed.

seim - Today 2:51 PM

SIEM
sshd: authentication failed.

seim - Today 2:51 PM

SIEM
sshd: authentication failed.

SIEM APP
Today at 2:51 PM

Host Blocked

Host Blocked by firewall-drop Active Response

2024/02/01 14:51:18 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"node01","module":"wazuh-execd"},"command":"add","parameters":{"extra_args":"","alert":{"timestamp":"2024-02-01T14:51:18.490+0700","rule":{"level":10,"description":"IP address 58.11.15.160 trying to Brute Force","id":"100030","frequency":4,"firedtimes":2,"mail":false,"groups":["local","syslog","sshd","authentication_failed"],"pgp13":["7.1"]},"agent":{"id":"003","name":"WWW","ip":"172.31.45.16"},"manager":{"name

Show more...

Host
(003) - WWW

Rule ID
651 (Level 3)
Today at 2:51 PM

ภาพประกอบที่ ก.9 แจ้งเตือน100030ทดสอบครั้งที่ 4

Messages 22

Files 0

Sort: Newest

From

In

Only my ch

seim - Today 3:40 PM

SIEM

Host Blocked by firewall-drop Active Response

seim - Today 3:40 PM

SIEM

IP address [?]58.11.15.160 trying to Brute Force.

seim - Today 3:40 PM

SIEM

sshd: authentication failed.

seim - Today 3:40 PM

SIEM

sshd: authentication failed.

seim - Today 3:40 PM

SIEM

sshd: authentication failed.

SIEM APP

Today at 3:40 PM

Host Blocked

Host Blocked by firewall-drop Active Response

2024/02/01 15:40:04 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"node01","module":"wazuh-execd"},"command":"add","parameters":{"extra_args":[],"alert":{"timestamp":"2024-02-01T15:40:04.760+0700","rule":{"level":10,"description":"IP address 58.11.15.160 trying to Brute Force","id":"100030","frequency":4,"firedtimes":1,"mail":false,"groups":["local","syslog","sshd","authentication_failed"],"pgp13":["7.1"]},"agent":{"id":"003","name":"WWW","ip":"172.31.45.16"},"manager":{"name

Show more...

Host

(003) - WWW

Rule ID

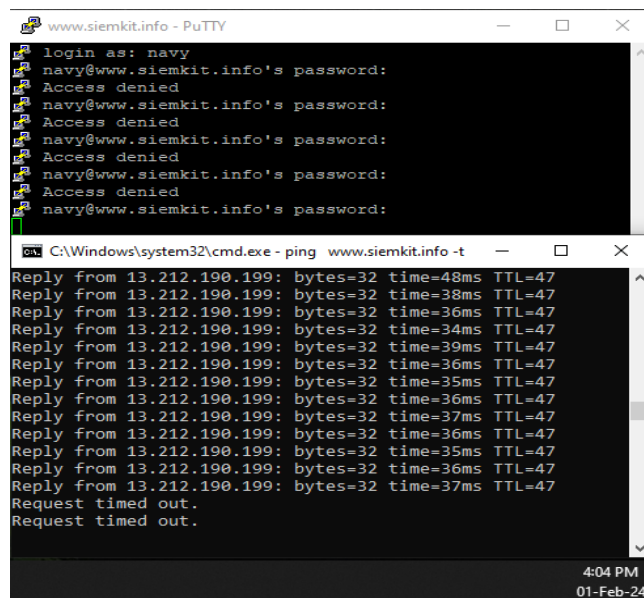
651 (Level 3)

Today at 3:40 PM

ภาพประกอบที่ ก.10 แจ้งเตือน 100030 ทดสอบครั้งที่ 5

2. การทดสอบตามเงื่อนไขที่ 100040

2.1 ทดสอบการวิเคราะห์และป้องกันบนเครื่องแม่ข่ายแบบเรียลไทม์



```

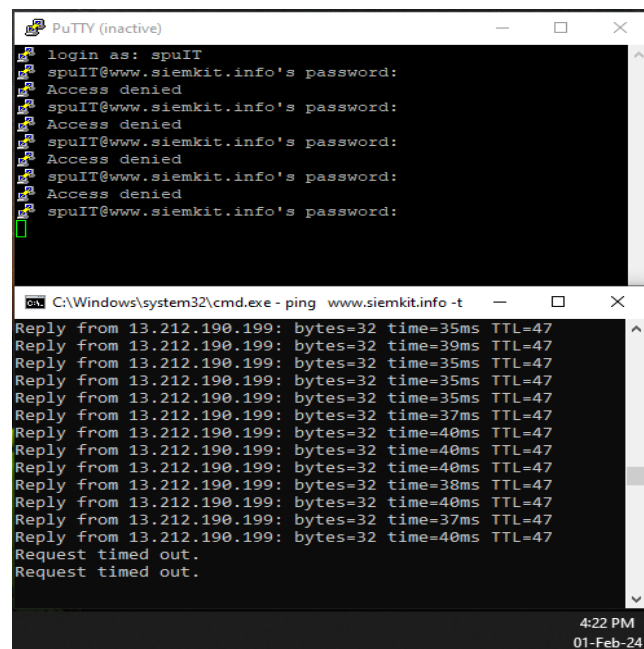
www.siemkit.info - PuTTY
login as: navy
navy@www.siemkit.info's password:
Access denied
navy@www.siemkit.info's password:
Access denied
navy@www.siemkit.info's password:
Access denied
navy@www.siemkit.info's password:
Access denied
navy@www.siemkit.info's password:

C:\Windows\system32\cmd.exe - ping www.siemkit.info -t
Reply from 13.212.190.199: bytes=32 time=48ms TTL=47
Reply from 13.212.190.199: bytes=32 time=38ms TTL=47
Reply from 13.212.190.199: bytes=32 time=36ms TTL=47
Reply from 13.212.190.199: bytes=32 time=34ms TTL=47
Reply from 13.212.190.199: bytes=32 time=39ms TTL=47
Reply from 13.212.190.199: bytes=32 time=36ms TTL=47
Reply from 13.212.190.199: bytes=32 time=35ms TTL=47
Reply from 13.212.190.199: bytes=32 time=36ms TTL=47
Reply from 13.212.190.199: bytes=32 time=37ms TTL=47
Reply from 13.212.190.199: bytes=32 time=36ms TTL=47
Reply from 13.212.190.199: bytes=32 time=35ms TTL=47
Reply from 13.212.190.199: bytes=32 time=36ms TTL=47
Request timed out.
Request timed out.

4:04 PM
01-Feb-24

```

ภาพประกอบที่ ก.11 เงื่อนไขที่ 100040 ทดสอบครั้งที่ 1



```

PuTTY (inactive)
login as: spuIT
spuIT@www.siemkit.info's password:
Access denied
spuIT@www.siemkit.info's password:
Access denied
spuIT@www.siemkit.info's password:
Access denied
spuIT@www.siemkit.info's password:
Access denied
spuIT@www.siemkit.info's password:

C:\Windows\system32\cmd.exe - ping www.siemkit.info -t
Reply from 13.212.190.199: bytes=32 time=35ms TTL=47
Reply from 13.212.190.199: bytes=32 time=39ms TTL=47
Reply from 13.212.190.199: bytes=32 time=35ms TTL=47
Reply from 13.212.190.199: bytes=32 time=35ms TTL=47
Reply from 13.212.190.199: bytes=32 time=35ms TTL=47
Reply from 13.212.190.199: bytes=32 time=37ms TTL=47
Reply from 13.212.190.199: bytes=32 time=40ms TTL=47
Reply from 13.212.190.199: bytes=32 time=40ms TTL=47
Reply from 13.212.190.199: bytes=32 time=38ms TTL=47
Reply from 13.212.190.199: bytes=32 time=40ms TTL=47
Reply from 13.212.190.199: bytes=32 time=37ms TTL=47
Reply from 13.212.190.199: bytes=32 time=40ms TTL=47
Request timed out.
Request timed out.

4:22 PM
01-Feb-24

```

ภาพประกอบที่ ก.12 เงื่อนไขที่ 100040 ทดสอบครั้งที่ 2

A screenshot of a PuTTY terminal window titled "PuTTY (inactive)". The terminal shows several failed login attempts from MSIT28@www.siemkit.info's machine. Each attempt consists of a password prompt followed by "Access denied". At the bottom, there are four network-related messages indicating replies from 13.212.190.199 with varying times and TTL values, followed by two "Request timed out." messages.

```
PuTTY (inactive)
login as: MSIT28
MSIT28@www.siemkit.info's password:
Access denied
MSIT28@www.siemkit.info's password:
Access denied
MSIT28@www.siemkit.info's password:
Access denied
MSIT28@www.siemkit.info's password:
Access denied
MSIT28@www.siemkit.info's password:
Access denied
Reply from 13.212.190.199: bytes=32 time=3/ms TTL=47
Reply from 13.212.190.199: bytes=32 time=36ms TTL=47
Reply from 13.212.190.199: bytes=32 time=33ms TTL=47
Reply from 13.212.190.199: bytes=32 time=44ms TTL=47
Request timed out.
Request timed out.
```

5:01 PM
01-Feb-2

ภาพประกอบที่ ก.15 เงื่อนไขที่100040ทดสอบครั้งที่ 5

2.2 ทดสอบการวิเคราะห์และแจ้งเตือนภัยคุกคามบนเครื่องแม่ข่ายแบบเรียลไทม์

The screenshot displays a SIEM interface with a list of alerts on the left and a detailed view of a 'Host Blocked' alert on the right. The alerts on the left are all from the source '# seim - Today' at '4:04 PM', indicating 'ssh: Attempt to login using a non-existent user' from IP address 58.11.15.160. The detailed view on the right shows the alert was triggered by a 'firewall-drop Active Response' at '2024/02/01 16:04:46'. It includes technical details such as the rule level (10), description, and agent information (id: 003, name: WWW).

ภาพประกอบที่ ก.16 แจ้งเตือน100040ทดสอบครั้งที่ 1

This screenshot shows the SIEM interface with a list of alerts on the left and a detailed view of a 'Host Blocked' alert on the right. The alerts on the left are from the source '# seim - Today' at '4:22 PM', indicating 'ssh: Attempt to login using a non-existent user' from IP address 58.11.15.160. The detailed view on the right shows the alert was triggered by a 'firewall-drop Active Response' at '2024/02/01 16:22:24'. It includes technical details such as the rule level (10), description, and agent information (id: 003, name: WWW).

ภาพประกอบที่ ก.17 แจ้งเตือน100040ทดสอบครั้งที่ 2

Messages 42 Files 0

Sort: Newest From In Only my ch

seim - Today 4:35 PM

SIEM
Host Blocked by firewall-drop Active Response

seim - Today 4:35 PM

SIEM
sshd: Attempt to login using a non-existent user

seim - Today 4:35 PM

SIEM
IP address [?] 58.11.15.160 🚫 sshd: Attempt to login using a non-existent user.

seim - Today 4:35 PM

SIEM
sshd: Attempt to login using a non-existent user

seim - Today 4:35 PM

SIEM
sshd: Attempt to login using a non-existent user

SIEM APP
Today at 4:35 PM

Host Blocked

Host Blocked by firewall-drop Active Response

2024/02/01 16:35:19 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"node01","module":"wazuh-execd"},"command":"add","parameters":{"extra_args":[],"alert":{"timestamp":"2024-02-01T16:35:19.651+0700","rule":{"level":10,"description":"IP address 58.11.15.160 sshd: Attempt to login using a non-existent user","id":"100040","frequency":5,"firedtimes":3,"mail":false,"groups":["local","syslog","sshd","syslog","sshd","authentication_failed","invalid_login"]},"agent":{"id":"003","nam

[Show more...](#)

Host
(003) - WWW

Rule ID
651 (Level 3)

Today at 4:35 PM

ภาพประกอบที่ ก.18 แจ้งเตือน 100040 ทดสอบครั้งที่ 3

Messages 49 Files 0

Sort: Newest From In Only my ch

seim - Today 4:49 PM

SIEM
Host Blocked by firewall-drop Active Response

seim - Today 4:49 PM

SIEM
sshd: Attempt to login using a non-existent user

seim - Today 4:49 PM

SIEM
IP address [?] 58.11.15.160 🚫 sshd: Attempt to login using a non-existent user.

seim - Today 4:49 PM

SIEM
sshd: Attempt to login using a non-existent user

seim - Today 4:49 PM

SIEM
sshd: Attempt to login using a non-existent user

SIEM APP
Today at 4:49 PM

Host Blocked

Host Blocked by firewall-drop Active Response

2024/02/01 16:49:26 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"node01","module":"wazuh-execd"},"command":"add","parameters":{"extra_args":[],"alert":{"timestamp":"2024-02-01T16:49:26.490+0700","rule":{"level":10,"description":"IP address 58.11.15.160 sshd: Attempt to login using a non-existent user","id":"100040","frequency":5,"firedtimes":4,"mail":false,"groups":["local","syslog","sshd","syslog","sshd","authentication_failed","invalid_login"]},"agent":{"id":"003","nam

[Show more...](#)

Host
(003) - WWW

Rule ID
651 (Level 3)

Today at 4:49 PM

ภาพประกอบที่ ก.19 แจ้งเตือน 100040 ทดสอบครั้งที่ 4

Messages 56 Files 0

Sort: Newest From In Only my ch

seim - Today 5:01 PM

SIEM
Host Blocked by firewall-drop Active Response

seim - Today 5:01 PM

SIEM
IP address 58.11.15.160 sshd: Attempt to login using a non-existent user.

seim - Today 5:01 PM

SIEM
sshd: Attempt to login using a non-existent user

seim - Today 5:01 PM

SIEM
sshd: Attempt to login using a non-existent user

seim - Today 5:01 PM

SIEM
sshd: Attempt to login using a non-existent user

SIEM APP
Today at 5:01 PM

Host Blocked

Host Blocked by firewall-drop Active Response

2024/02/01 17:01:31 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"node01","module":"wazuh-execd"},"command":"add","parameters":{"extra_args":"","alert":{"timestamp":"2024-02-01T17:01:30.995+0700","rule":{"level":10,"description":"IP address 58.11.15.160 sshd: Attempt to login using a non-existent user","id":"100040","frequency":5,"firedtimes":1,"mail":false,"groups":["local","syslog","sshd","syslog","sshd","authentication_failed","invalid_login"]},"agent":{"id":"003","nam

Show more...

Host
(003) - WWW

Rule ID
651 (Level 3)

Today at 5:01 PM

ภาพประกอบที่ ก.20 แจ้งเตือน100040ทดสอบครั้งที่ 5

ภาคผนวก ข

คู่มือการใช้งานแอปพลิเคชัน SIEMKIT

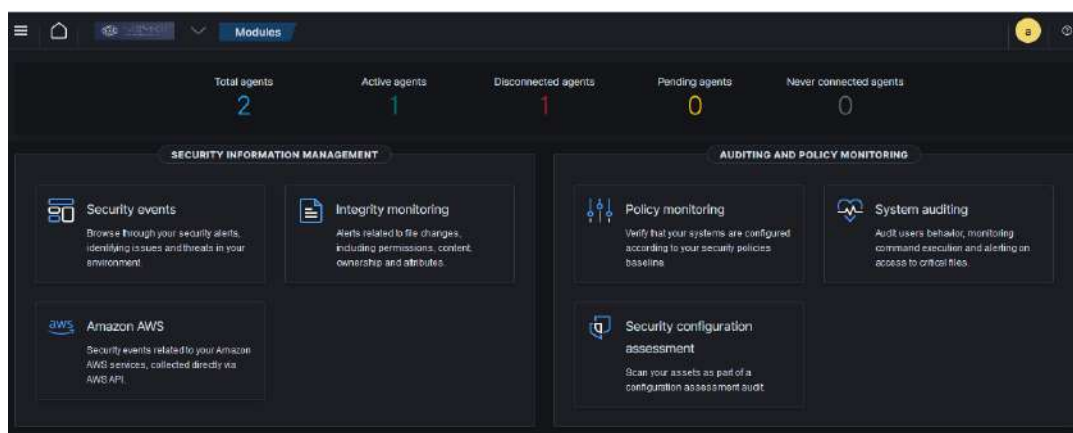
1. การใช้งานระบบแอปพลิเคชัน

1.1 การเข้าถึงการใช้งานระบบ SIEMKIT สามารถใช้งานได้โดยผ่านเบราว์เซอร์ตามลิงค์ดังนี้ <https://xdr.siemkit.com> ซึ่งหน้าจอระบบจะแสดงดังรูปข้างล่างนี้



ภาพประกอบที่ ข.1 หน้าล็อกอินเข้าสู่ระบบ SIEM

1.2 เมื่อกรอกข้อมูลได้ถูกต้องจากการเข้าสู่ระบบ ระบบจะแสดงหน้าจอ Dashboard ของข้อมูลระบบ SIEM และจะแสดงเมนูต่างๆ ดังรูปที่ ข.2



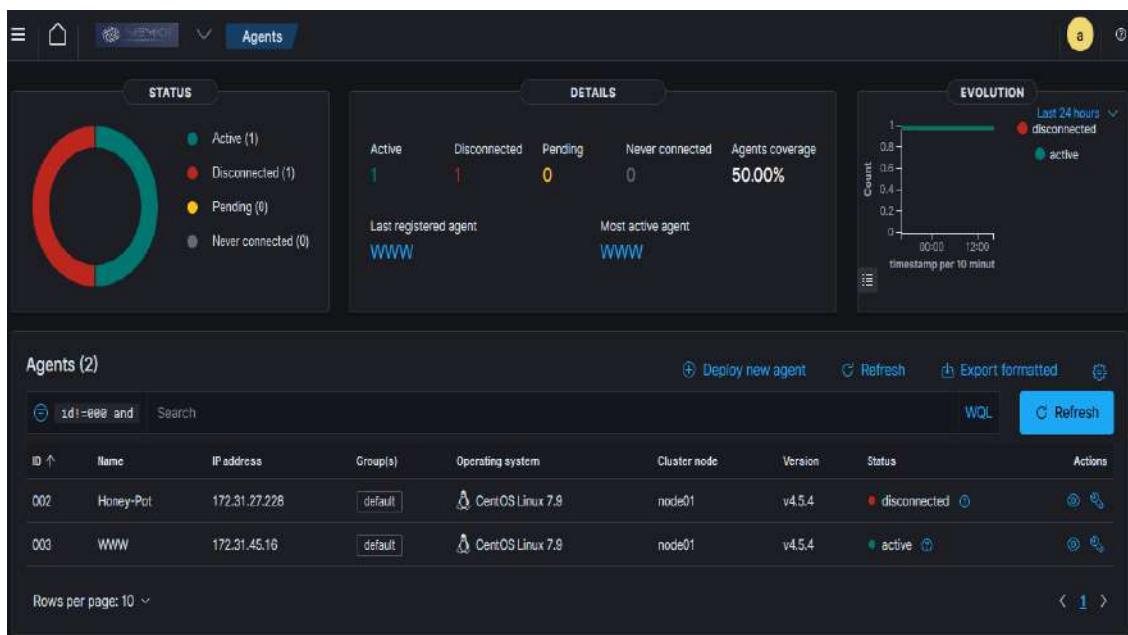
ภาพประกอบที่ ข.2 แสดงหน้าจอ Dashboard ของข้อมูลระบบ SIEM

1.3 ผู้ใช้งานสามารถเห็นแสดงค่าการทำงานของ Agent ที่ติดตั้งในเครื่องคอมพิวเตอร์แม่ข่ายว่าทำงานหรือไม่ทำงานอยู่กี่รายการ ดังภาพประกอบที่ ข.3



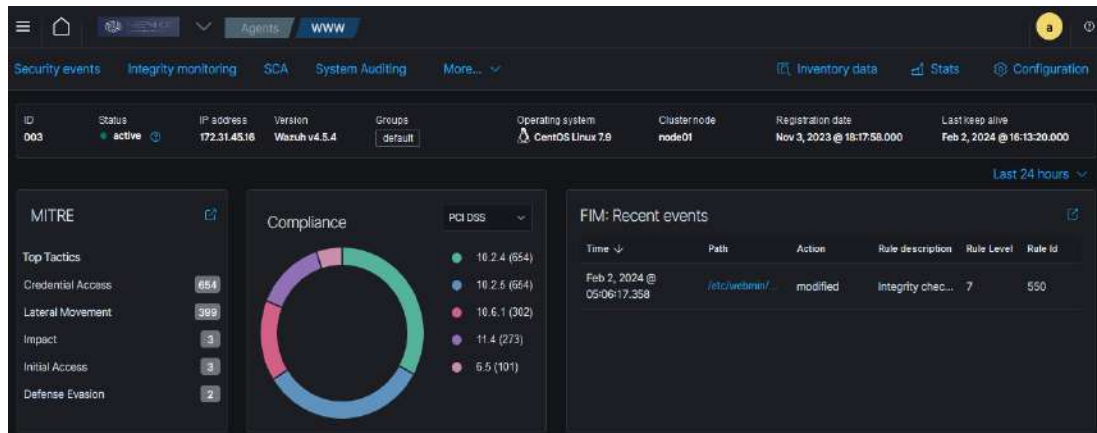
ภาพประกอบที่ ข.3 แสดงค่าสถานะของ Agent ที่ติดตั้ง

1.4 ผู้ใช้งานกดเลือกเมนู Total Agent เพื่อดูรายละเอียดของเครื่องคอมพิวเตอร์แม่ข่ายที่ Agent ที่ทำงานอยู่มีรายละเอียดเป็นอย่างไร ดังภาพประกอบที่ ข.4



ภาพประกอบที่ ข.4 แสดงรายละเอียดของเครื่องคอมพิวเตอร์แม่ข่ายที่ Agent ที่ทำงานอยู่

1.5 ผู้ใช้งานกดเลือกรายการ Agent ที่อยู่ตามรายการด้านล่างการสามารถไปส่วนรายละเอียดของเครื่องแม่ๆ นั้นที่ Agent ทำงานอยู่ ซึ่งจะแสดงในส่วนการวิเคราะห์เหตุการณ์ที่ตรวจพบในกิจกรรมตามรายละเอียด ดังภาพประกอบที่ ข.5



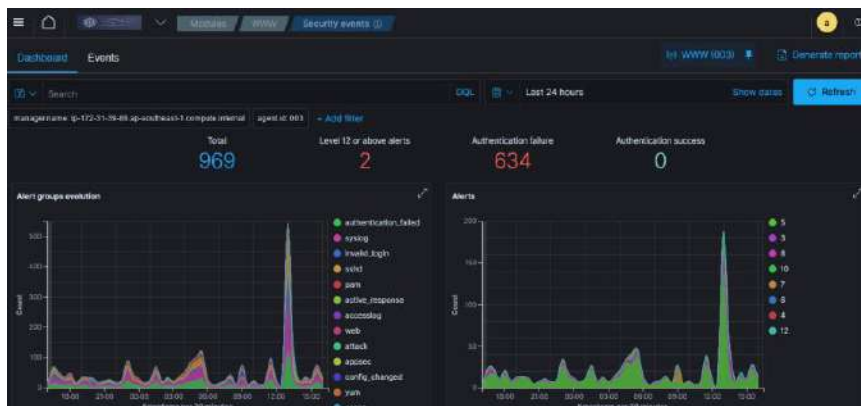
ภาพประกอบที่ ข.5 แสดงในส่วนการวิเคราะห์เหตุการณ์ที่ตรวจพบเครื่องคอมพิวเตอร์แม่ข่าย

1.6 รายละเอียดที่จากการบันทึกหน้ารายการจะแสดงข้อมูลที่จะจัดเก็บล่าสุดภายใน 24 ชม. และนำมาเปรียบเทียบกับค่าของ MITRE, PCI DSS, GDPR, NIST 800-53 เป็นต้น



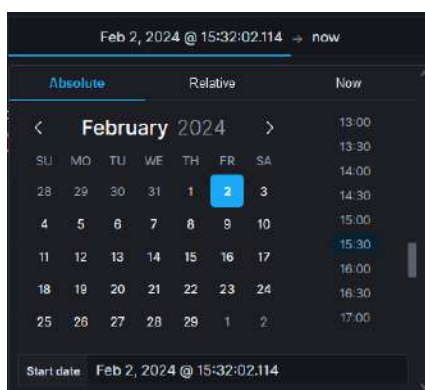
ภาพประกอบที่ ข.6 แสดงค่าเปรียบเทียบกับ MITRE, PCI DSS, GDPR, NIST 800-53

1.7 เมื่อผู้ใช้งานทำการเลือกเมนูด้านซ้ายบน หัวข้อ Security events จะเข้าสู่หน้ารายการแสดง Dashboard ของส่วน Security events ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่าย โดยหน้านี้จะแสดงรายเอียดเหตุการณ์ที่เกิดขึ้นในภัยคุกคาม ในช่วง 24 ชม. ที่ผ่านมา ตามภาพประกอบที่ ข.7



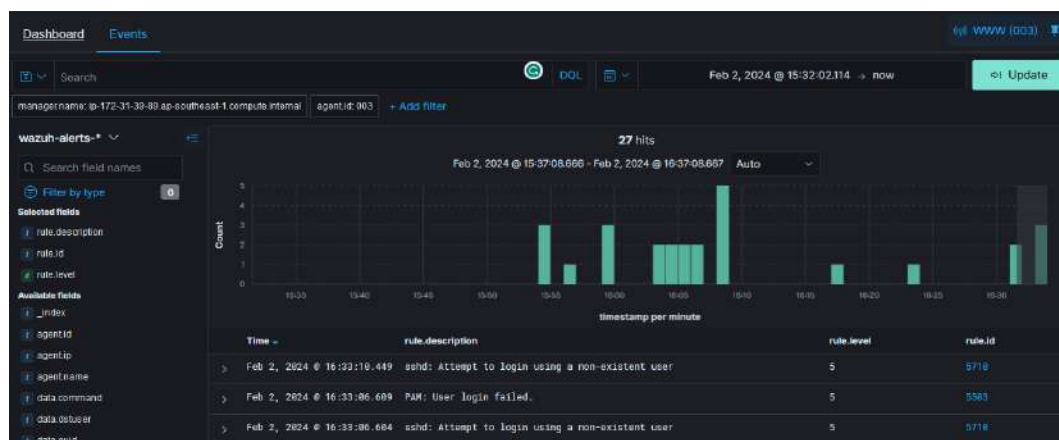
ภาพประกอบที่ ข.7 แสดงรายเอียดเหตุการณ์ที่เกิดขึ้นในภัยคุกคามที่เข้าเครื่องคอมพิวเตอร์แม่ข่าย

1.8 ผู้ใช้งานสามารถเลือกช่วงเวลาที่จะตรวจกิจกรรมในเครื่องแม่ได้โดยการเลือกเมนู รูปตาราง ปฏิทิน หรือ Show Dates เพื่อระบบช่วงเวลาที่ต้อง จากนั้นกดเมนู Refresh เพื่อแสดงค่าตามช่วงเวลา กำหนดนำมาแสดง



ภาพประกอบที่ ข.8 แสดง Show Dates เพื่อระบบช่วงเวลาที่ต้อง

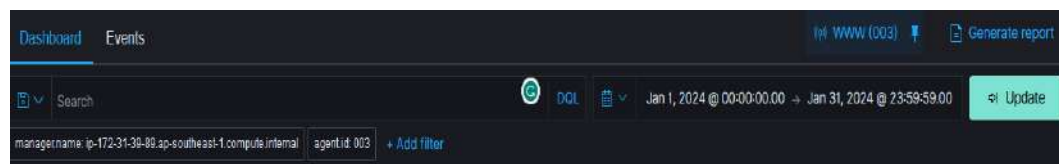
1.9 ผู้ใช้งานทำการกดเมนู Events จากหน้า Dashboard ของส่วน Security events เข้าไปจะพบหน้ารายการ Log จากเครื่องคอมพิวเตอร์แม่ข่ายที่นำมาบันทึกกิจกรรม ที่เกิดขึ้นและแสดงในรูปแบบรายการ List เพื่อสามารถดูรายการที่เกิดขึ้นอย่างละเอียดเช่น วันเวลาเกิดเหตุ เกิดเหตุการณ์ใด ประเภทของภัยคุกคาม และเลขหมายต้องกับกำหนดเงื่อนไข พร้อมทั้งแสดงเป็นกราฟ



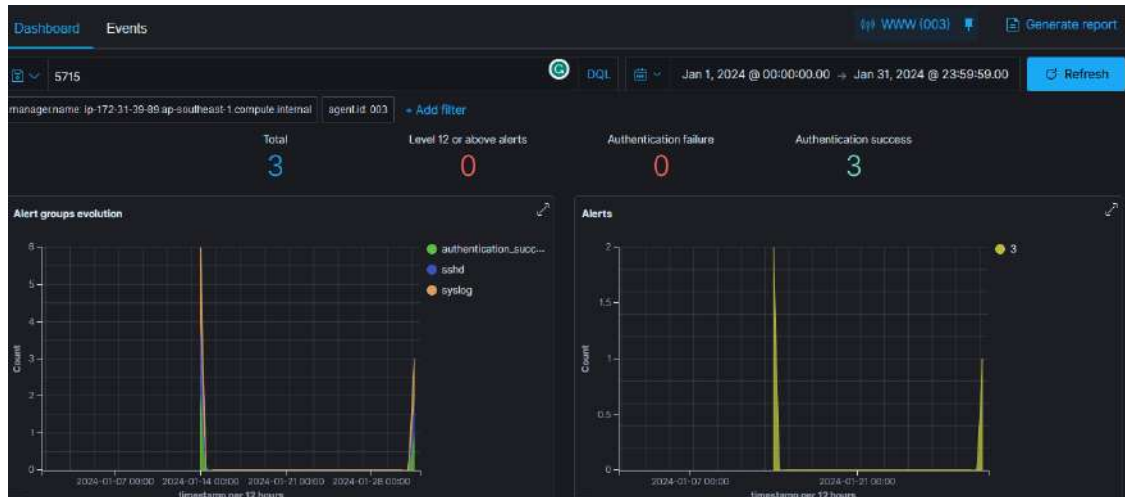
ภาพประกอบที่ ข.9 แสดง Show Dates เพื่อระบบช่วงเวลาที่ต้อง

2. การค้นหาข้อมูลและสร้างรายงานเพื่อใช้ในการวิเคราะห์

2.1 ผู้ใช้งานเข้าสู่หน้าการทำงานของ Dashboard ของส่วน Security events จากนั้นให้พิมพ์ข้อความที่จะค้นหาหรือ rule.id ในช่องว่าง ที่คำว่า Search และกำหนดช่วงเวลาที่ต้องการค้นหา แล้วกด เมนูUpdate จากนั้นจะแสดงค่าจำนวนรายการที่เกิดขึ้นในช่วงเวลาที่กำหนด พร้อมกราฟ เพื่อใช้ในการวิเคราะห์



ภาพประกอบที่ ข.10 แสดง Search และกำหนดช่วงเวลาที่ต้องการค้นหา



ภาพประกอบที่ ข.11 แสดงค่าการค้นหาคำหนดไว้

2.2 เมื่อผู้ใช้ค้นหาได้ข้อมูลตรงตามต้องการแล้ว สามารถสร้างรายงานได้โดยการเลือกเมนูชื่อ Generate report เพื่อสั่งให้ระบบ SIEM สร้างรายงานออกมาเป็นไฟล์ PDF รายงาน จากนั้นให้กดเลือกสัญลักษณ์ ^ แถบบาร์ด้านบนจากนั้นเลือก เมนู Management -> Reporting ก็จะเข้าสู่ส่วนหน้า Reporting เพื่อดาวน์โหลดไฟล์รายงานที่สร้างไว้ โดยเลือกไฟล์รายงานที่ต้องการ จากนั้นเลือกสัญลักษณ์ไอคอนสีฟ้า เพื่อกดดาวน์โหลดไฟล์รายงาน ดังภาพประกอบที่ ข.13

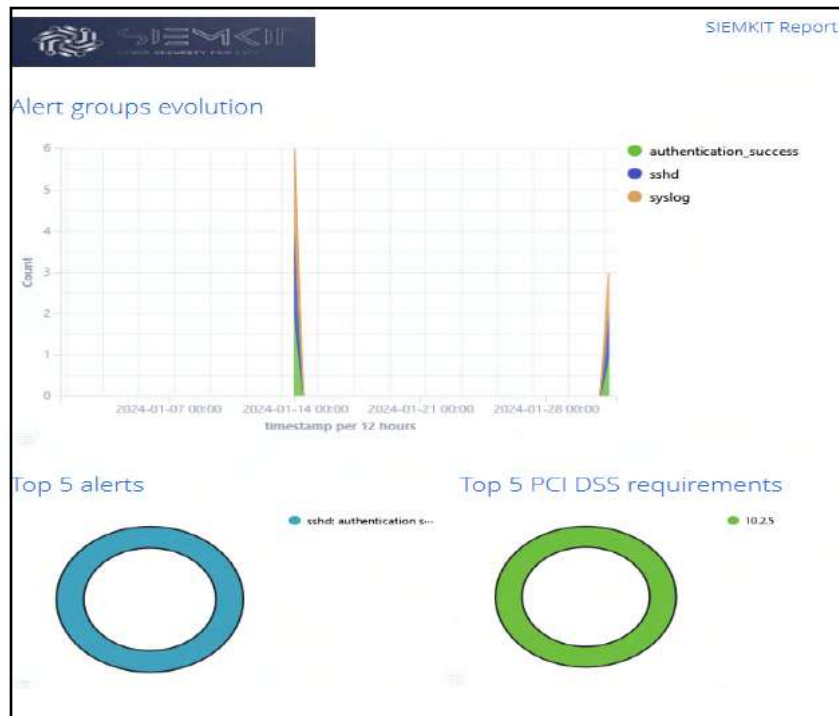
The screenshot shows the 'Reporting' page in the Wazuh dashboard. It contains a table with the following data:

File	Size	Created ↓	Actions
wazuh-module-agents-003-general-1706668717.pdf	90.33KB	Feb 2, 2024 @ 17:11:58.337	
wazuh-module-agents-003-general-1706714445.pdf	197.03KB	Jan 31, 2024 @ 22:20:48.854	
wazuh-module-agents-003-general-1690530782.pdf	170.89KB	Nov 9, 2023 @ 18:52:43.365	

ภาพประกอบที่ ข.12 แสดงหน้า Reporting เพื่อดาวน์โหลดรายงาน



ภาพประกอบที่ ข.13 แสดงตัวอย่างรายงานที่สร้างจากระบบ SIEM



ภาพประกอบที่ ข.14 แสดงตัวอย่างค่าการวิเคราะห์ห้อย่างรายงานระบบ SIEM

ภาคผนวก ค

ใบตอบรับการตีพิมพ์และวารสารที่ได้รับการตีพิมพ์

18 เมษายน 2567

เรื่อง ตอบรับลงบทความวิจัย

เรียน คุณกฤษ ศรีเงินดี

ตามที่ คุณกฤษ ศรีเงินดี หลักสูตรวิทยาศาสตร์มหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม ได้ส่งบทความวิจัย เรื่อง “การพัฒนาแบบติดตาม เฝ้าระวัง และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคของการวิเคราะห์เหตุการณ์ตอบสนองแบบเรียลไทม์” เพื่อตีพิมพ์ในวารสารวิทยาศาสตร์และเทคโนโลยีแห่งรัตนโกสินทร์

กองบรรณาธิการ มีความยินดีรับบทความวิจัยของท่านเพื่อเผยแพร่ในวารสารวิทยาศาสตร์และเทคโนโลยีแห่งรัตนโกสินทร์ ปีที่ 6 ฉบับที่ 2 (พฤษภาคม - สิงหาคม 2567)

จึงเรียนมาเพื่อทราบ

ขอแสดงความนับถือ



(รองศาสตราจารย์ ดร.พิชิต กิตติสุวรรณ)

บรรณาธิการวารสารวิทยาศาสตร์และเทคโนโลยีแห่งรัตนโกสินทร์
มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์



Rajamangala University of Technology Rattanakosin
96 M.3 Phutthamonthon Sai 5 Rd., Salaya,
Phutthamonthon, Nakhonpathom, 73170, Thailand
E-mail: rjst@wmutrac.th Tel.+66 2441 6059

การพัฒนาระบบติดตาม เฝ้าระวัง และแจ้งเตือนภัยคุกคามทาง

ไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิค

ของการวิเคราะห์เหตุการณ์ตอบสนองแบบเรียลไทม์

Developing a system for tracking, monitoring, and alerting to
cyber threats on server computer using techniques of real-time
event analysis and response

กฤษ ศรีเงินดี^{1*} ประสงค์ ปราณีตพลกรัง² และ สุรศักดิ์ มั่งสิงห์³

^{1*, 2, 3} หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

E-mail: ¹kit.sringendee@gmail.com

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์ เพื่อพัฒนาระบบที่สามารถแจ้งเตือนภัยคุกคามทางไซเบอร์ประเภทการ
สุมหรือคาคตาที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายหรือเซิร์ฟเวอร์ ที่มีให้บริการการเข้าถึงข้อมูลจาก
ภายนอกองค์กร ทั้งนี้ ระบบที่พัฒนาขึ้นได้ทำการแจ้งเตือนให้ผู้ดูแลเครื่องเซิร์ฟเวอร์ด้วยเวลาที่ใกล้เคียงกับ
เวลาจริงหรือเรียลไทม์ เพื่อที่จะยับยั้งความเสียหายอันเกิดขึ้นกับเครื่องเซิร์ฟเวอร์ และกำกับดูแลได้อย่าง
ต่อเนื่องหากมีการบุกรุกทางไซเบอร์ที่อาจเกิดขึ้นได้ในเวลาใด ๆ ผลการวิจัยพบว่า การโจมตีเครื่องเซิร์ฟเวอร์
ประเภทการสุมหรือคาคตา นั้น ผู้วิจัยใช้ระบบติดตาม เฝ้าระวัง และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่อง
คอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองแบบเรียลไทม์ที่พัฒนาขึ้น สามารถ
วิเคราะห์ติดตามและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องเซิร์ฟเวอร์ ได้มีประสิทธิภาพอยู่ในระดับมาก
ที่สุด ($\bar{X} = 5.00$)

คำสำคัญ : การแจ้งเตือน, ภัยคุกคามทางไซเบอร์, คอมพิวเตอร์แม่ข่าย

* Corresponding author, e-mail: kit.sringendee@gmail.com

Submission date: 19/02/ 2024 Revised date: 13/04/2024 Accepted date: 18/04/2024

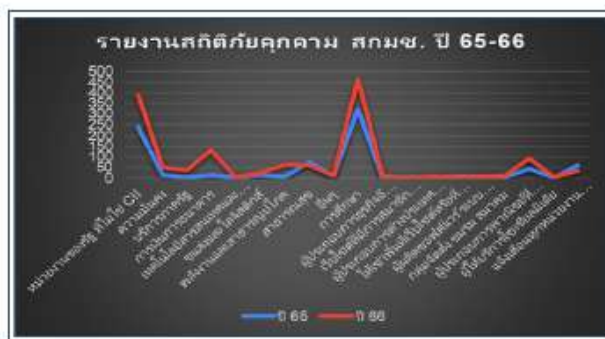
Abstract

This research aims to develop a system that can warn of cyber threats such as simple brute force attacks that occur on host computers or servers which provides access to data from outside the organization. Therefore, the developing system has alerted server computer administrators to receive information in near real-time notifications. Then, it can be able to prevent damage from cyber intrusion and continuously supervise the server computer at any time of the cyber attack. The research result found that in brute force attacks on servers, researchers use the developed system such as a system for tracking, monitoring, and alerting to cyber threats on servers using real-time event analysis and response techniques to monitor, detect, analyze, and alert to server computer administrators before any cyber attacker can harm the organization in real time with the highest efficiency ($\bar{X} = 5.00$)

Keywords: Alert, Cyber Threat, Server.

1. บทนำ

ปัจจุบันมีการใช้บริการผ่านอินเทอร์เน็ตอย่างแพร่หลายอันส่งผลให้มีผู้ไม่หวังดีที่ต้องการแสวงหาผลประโยชน์จากข้อมูลของผู้ใช้งานในระบบอินเทอร์เน็ต และต้องการเข้าถึงระบบแม่ข่ายของผู้ให้บริการ ซึ่งก่อให้เกิดความเสียหายแก่ผู้ให้บริการและผู้ใช้บริการ ตามสถิติของ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ดังรูปที่ 1 [1] พบว่าในปี 2565 มีรายงานภัยคุกคามทางไซเบอร์จำนวน 835 รายการ และในปี 2566 มีจำนวน 1,789 รายการ เพิ่มขึ้นถึง 214.2% แสดงให้เห็นว่าในปัจจุบันภัยคุกคามทางไซเบอร์มีอัตราการเติบโตอย่างต่อเนื่อง องค์กรต่าง ๆ ควรให้ความสำคัญกับภัยคุกคามทางไซเบอร์มากขึ้น



รูปที่ 1 รายงานสถิติภัยคุกคาม สกมช. ประจำปี พ.ศ. 2565-2566

ปัจจุบันระบบการตรวจหา วิเคราะห์ และตอบสนองต่อภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ (Security Information and Event Management : SIEM) เป็นทางออกหรือการแก้ปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ โดยทำการรวบรวมข้อมูลเหตุการณ์จากแหล่งต่าง ๆ มาวิเคราะห์แบบทันทีทันใดหรือเรียลไทม์ (Real-Time) เพื่อตรวจจับกิจกรรมที่ผิดปกติ เมื่อนำ SIEM มาใช้ร่วมกับ Application Slack ที่เป็นแพลตฟอร์มการสื่อสารภายในองค์กรแล้วจะช่วยให้สมาชิกติดต่อสื่อสารกันผ่านข้อความ ผ่านการโทรศัพท์ หรือการแชร์ไฟล์ได้สะดวกมากขึ้น ดังนั้นการนำ SIEM มาใช้จะช่วยในการตรวจสอบ วิเคราะห์ และแจ้งเตือนภัยคุกคามทางไซเบอร์แบบเรียลไทม์จะช่วยเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยของคอมพิวเตอร์แม่ข่ายในองค์กรได้มากยิ่งขึ้น

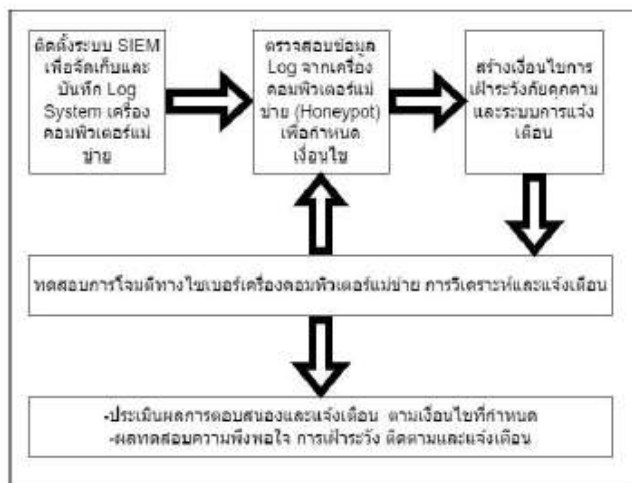
2. วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาวิเคราะห์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่าย
2. เพื่อพัฒนาระบบการแจ้งเตือนเมื่อเกิดภัยคุกคามแบบ Simple Brute Force Attacks อย่างเรียลไทม์
3. เพื่อทำการประเมินประสิทธิภาพการวิเคราะห์และแจ้งเตือนภัยคุกคามทางไซเบอร์แบบ Simple Brute Force Attacks อย่างเรียลไทม์

3. กรอบแนวความคิดในการวิจัย

การวิจัยนี้ เป็นการพัฒนาระบบการแจ้งเตือนภัยคุกคามทางไซเบอร์ของเครื่องคอมพิวเตอร์แม่ข่าย โดยการโจมตีแบบ SSH Network Protocol แบบสุ่มรหัสผ่านผู้ดูแลระบบแบบเรียลไทม์ด้วยการกำหนดเงื่อนไขตามที่ผู้พัฒนาได้กำหนดและใช้ค่าเปรียบเทียบกับ MITRE ATT&CK Framework [2] โดยผู้วิจัยได้กำหนดกรอบแนวความคิดในการวิจัยดังรูปที่ 2 และมีขอบเขตของการวิจัย ดังนี้

1. การพัฒนาการวิเคราะห์ข้อมูลเหตุการณ์ (Log System) บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์เปรียบเทียบกับ MITRE ATT&CK Framework
2. ขอบเขตการวิเคราะห์จากการเทคนิคการสุ่มรหัสผ่านแบบ Simple Brute Force Attacks [3] ผ่านช่องทางการเชื่อมต่อแบบ Secure Shell (SSH) และ port 22
3. การแจ้งเตือนเมื่อเกิดภัยคุกคามแบบเรียลไทม์จะมีระยะใกล้เคียงเหตุการณ์ใกล้เคียงที่สุดตามระยะที่เครื่องคอมพิวเตอร์แม่ข่าย ส่งผ่านข้อมูลมายังระบบ SIEM
4. ระยะเวลาที่ใช้เก็บข้อมูล Log System และวิเคราะห์การป้องกัน ตั้งแต่เดือน ตุลาคม 2566 ถึง มกราคม 2567



รูปที่ 2 กรอบแนวความคิดในการวิจัย

4. วิธีดำเนินการวิจัย

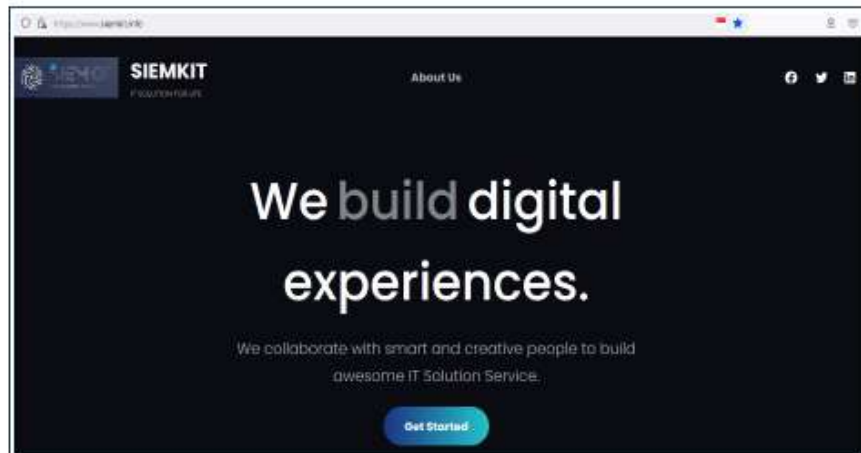
การวิจัยครั้งนี้ เป็นการวิจัยและพัฒนา (Research and Development) ตามขั้นตอนดังต่อไปนี้

ขั้นตอนที่ 1 การศึกษาเอกสารแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

- 1) การทำงานของระบบ SIEM ในการรับข้อมูล Log System จากเครื่องคอมพิวเตอร์แม่ข่าย
- 2) การแจ้งเตือนระบบผ่าน Application Slack โดยการใช้การเปรียบเทียบ Log System กับเงื่อนไขการข้อมูลของ MITRE ATT&CK Framework ในฐานข้อมูลของระบบ SIEM
- 3) ใช้ภาษาไพทอน ในการอ่านข้อมูล Log ที่เขียนอยู่ในรูปแบบ JSON แล้วส่งข้อมูลมายังผู้ดูแลระบบ (Admin)

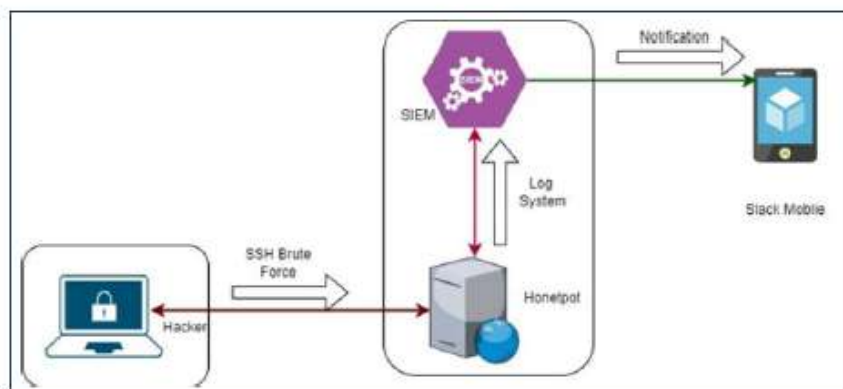
ขั้นตอนที่ 2 การจัดเก็บ Log System จากเครื่องคอมพิวเตอร์แม่ข่ายที่เป็นกับดักเพื่อลวงหรือเหยื่อล่อ (Honeypot) ที่ให้บริการผ่านช่องทางอินเทอร์เน็ต ได้มีการติดตั้งโปรแกรมการจัดเก็บ Log System โดยเครื่องคอมพิวเตอร์แม่ข่ายติดตั้งที่ AWS Cloud ดังรูปที่ 3

- 1) จัดเก็บข้อมูลการโจมตีแบบสุ่มรหัสผ่านทาง SSH port22 ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่าย
- 2) เปรียบเทียบกับเทคนิคการโจมตีในฐานข้อมูล MITRE ATT&CK Framework เพื่อทำเงื่อนไขการวิเคราะห์โจมตีเครื่องคอมพิวเตอร์แม่ข่ายและแจ้งเตือนผ่าน Application Slack
- 3) กำหนดรายละเอียดข้อมูลการแจ้งเตือนด้วยภาษาไพทอน (Python) ไปยัง Application Slack เพื่อให้ผู้ดูแลทราบถึงการแจ้งเตือน



รูปที่ 3 เครื่องคอมพิวเตอร์แม่ข่ายที่เป็นเหยื่อล่อ (Honeypot)

ขั้นตอนที่ 3 ประเมินประสิทธิภาพการวิเคราะห์และการแจ้งเตือนภัยคุกคามทางไซเบอร์แบบเรียลไทม์ โดยการทดสอบจำลองการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายโดยการคาดเดารหัสผ่าน ทาง SSH Port 22 เสมือนมีการโจมตีทางไซเบอร์ผ่านทาง Internet จากนั้นเก็บผลระยะเวลาที่ใช้ในการวิเคราะห์และแจ้งเตือนเพื่อประเมินประสิทธิภาพการตอบสนองการโจมตี ที่เกิดขึ้นกับการเครื่องคอมพิวเตอร์แม่ข่าย ที่เกิดขึ้น ตามกระบวนการทำงานที่ผู้วิจัยแสดง ดังรูปที่ 4



รูปที่ 4 Flow System Diagram

6 | กฤษฎา ศรีโพนทิ และคณะ

งานวิจัยนี้ ผู้วิจัยได้พัฒนาระบบติดตาม เฝ้าระวัง และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองแบบเรียลไทม์ ทั้งนี้ได้นำระบบ SIEM ประเภทหนึ่งที่มีชื่อ Wazuh เข้ามาใช้ในการจัดเก็บ Log จากเหตุการณ์การโจมตีเครื่องคอมพิวเตอร์แม่ข่าย โดย Wazuh Server ที่ทำงานร่วมกับ Elastic Stack เมื่อเกิดเหตุการณ์ขึ้นที่เครื่องคอมพิวเตอร์แม่ข่าย โปรแกรม Agent (beats) ที่ถูกติดตั้งไว้ที่เครื่องคอมพิวเตอร์แม่ข่าย จะส่งค่า Log มายัง Wazuh Server เพื่อมาทำการประมวลผลที่ Logstash แล้วจึงจัดเก็บที่ Elasticsearch ในรูปแบบ JSON ดังรูปที่ 5



รูปที่ 5 แสดงกระบวนการทำงาน Elastic Stack

จากนั้น Elasticsearch ที่อยู่ใน Wazuh Server จะทำการเปรียบเทียบกับกฎที่ผู้วิจัยได้กำหนดไว้ใน Rules ของ Wazuh Server ซึ่งอยู่ในรูปแบบคำสั่ง .XML ถ้าหากเกิดเหตุการณ์ การใส่รหัสผ่าน เป็นผู้ใช้ชื่อ Root ไม่ถูกต้อง ซึ่งตรงกับ Rule ID = 5760 แล้วหากเกิดซ้ำจำนวน 4 ครั้งด้วย IP ต้นทางเดียวกัน ภายใน 10 นาที ให้กำหนดเป็นการสุ่มหรือคาดเดา (Brute Force) จากนั้นเมื่อเหตุการณ์ใน Log ตรงกับกฎที่กำหนดไว้ เมื่อก่อนหน้านี้ก็ให้วิเคราะห์แบบพยายามสุ่มหรือคาดเดา และกำหนด Rule ID ใหม่เป็นค่า 100030 จากนั้นก็นำค่า 100030 ไปกำหนดเงื่อนไขของการแจ้งเตือนไปยังผู้ดูแลระบบด้วย Application Slack ต่อไป ดังรูปที่ 6

```

1 <!-- local rules -->
2
3 <!-- Modify it at your will. -->
4 <!-- Copyright (C) 2015, Wazuh Inc. -->
5
6 <!-- Example -->
7
8
9 <group name="local,aptlog,sahd">
10   <rule id="100030" level="10" frequency="4" timeframe="100">
11     <if watched_sids="5760"/> </if watched_sids>
12     <match source_ip />
13     <description>IP address $ip trying to Brute Force.</description>
14     <group>authentication.failed,apt3.7.1</group>
15   </rule>
16 </group>
17
  
```

รูปที่ 6 แสดงกำหนดกฎเงื่อนไขใน Wazuh Server

เมื่อผู้วิจัย ได้ค่าของ Rule ID แล้วก็นำค่าที่ได้มาเป็นเงื่อนไขในการกำหนดการแจ้งเตือนผู้ดูแลระบบ ด้วย Application Slack ผ่าน API โดยกำหนด พารามิเตอร์ใน Wazuh Server ในส่วนของคำสั่ง Integrates โดยจะไปส่งงานด้วยคำสั่งภาษาไพทอน ส่งรายละเอียดจาก Log ที่บันทึกในกฎ 100030 ไปยัง Slack API และ แสดงค่าที่ Application Slack ของผู้ดูแลระบบ ดังรูปที่ 7-8

```
<integration>
<name>custom-block</name>
<hook_url>https://hooks.slack.com/services/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</hook_url>
<rule_id>100030</rule_id>
<alert_format>json</alert_format>
</integration>
```

รูปที่ 7 แสดงพารามิเตอร์เงื่อนไขการแจ้งเตือน Wazuh Server

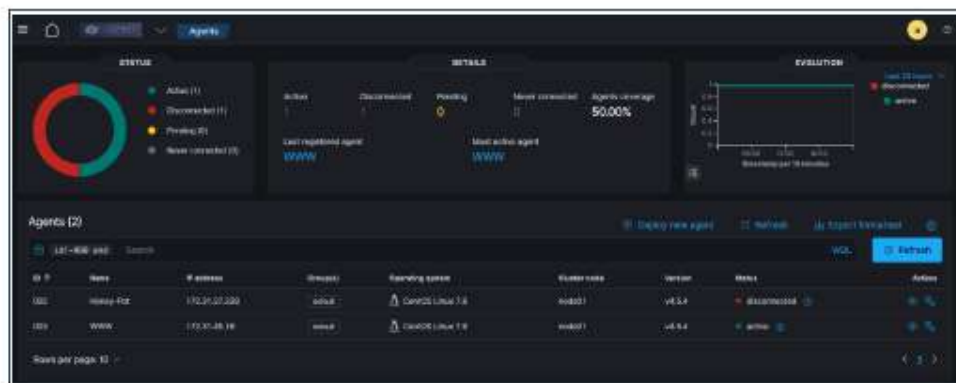
```
custom-block.py (/var/ossec/integrations)
def generate_msg(alert):
    level = alert['rule']['level']
    if (level <= 4):
        color = "good"
    elif (level == 5 and level <= 7):
        color = "warning"
    else:
        color = "danger"
    msg = {}
    msg['color'] = color
    msg['pretext'] = "Auto Block Alert"
    msg['title'] = alert['rule']['description'] if 'description' in alert['rule'] else "N/A"
    msg['text'] = alert.get('full_log')
    msg['fields'] = []
    if 'agent' in alert:
        msg['fields'].append({'title': "Host", 'value': "{0} - {1}".format(alert['agent']['id'], alert['agent']['name'])})
    msg['fields'].append({'title': "Rule ID", 'value': "{0} - {1}".format(alert['rule']['id'], level)})
    msg['ts'] = alert['id']
    attach = {'attachments': [msg]}
    return json.dumps(attach)
```

รูปที่ 8 แสดงคำสั่งไพทอนรายงานการโจมตีไปยัง Slack API

1. ระบบ SIEM Open Source (Wazuh) เป็นแพลตฟอร์มรักษาความมั่นคงปลอดภัยโอเพนซอร์ส ที่มีความสามารถในการจัดเก็บและรวบรวมเหตุการณ์ต่าง ๆ ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่าย จากการอ่านไฟล์ Log System ที่เกิดขึ้นในเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งโปรแกรม Agent ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์แม่ข่ายจะทำการอ่านและส่งข้อมูล Log มายังระบบ Wazuh Server เพื่อวิเคราะห์และแยกแยะข้อมูลออกเป็นส่วน ๆ เพื่อให้เข้าใจเหตุการณ์ที่เกิดขึ้น และรายละเอียดของเหตุการณ์ พร้อมทั้งเปรียบเทียบ

8 | กฤษฎา ศรีเงินทิ และคณะ

เหตุการณ์ที่เกิดขึ้นว่าเป็นภัยคุกคามกับ MITRE ATT&CK Framework หรือไม่ อีกทั้งสามารถนำค่าไปเปรียบเทียบกับกฎที่กำหนด เพื่อดำเนินการส่งชุดคำสั่งต่าง ๆ ได้ในเวลาเดียวกัน ซึ่งโดยแพลตฟอร์มแสดงการวิเคราะห์เหตุการณ์จาก Log System ที่เกิดขึ้นได้แบบเรียลไทม์ และสร้างรายงานเพื่อใช้ในการสรุปเหตุการณ์ตามช่วงเวลาได้อีกด้วย ตัวอย่างแสดงแดชบอร์ดอินเทอร์เฟซของระบบ Wazuh Server ดังรูปที่ 9



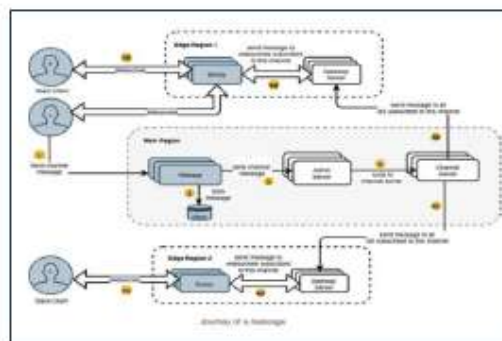
รูปที่ 9 แสดงแดชบอร์ดอินเทอร์เฟซผู้ใช้งานระบบ SIEM

2. กระบวนการจัดเก็บ Log System กระบวนการนี้ดำเนินการโดยซอฟต์แวร์เอเจนต์ (Agent) ติดตั้งที่เครื่องคอมพิวเตอร์แม่ข่ายซึ่งอ่านไฟล์บันทึกและกิจกรรมบนระบบปฏิบัติการหรือ Log ของแอปพลิเคชัน เช่น บันทึกการตรวจสอบระบบปฏิบัติการ Linux โดยรวบรวมเอาต์พุตและรายงานกลับไปยังเซิร์ฟเวอร์ Wazuh เพื่อการวิเคราะห์เพิ่มเติมโดยแสดงการเก็บ Log System ดังรูปที่ 10

The screenshot shows a list of security events in the Wazuh dashboard. The table has columns for 'Time', 'Rule description', 'Rule ID', and 'Status'. The events are listed in descending order of time, starting from '2024-06-15 00:00:00.000'. The events include 'Attempt to login using a non-existent user', 'User login failed', 'User login successful', and 'User login using a non-existent user'. The status of these events is 'Failed' or 'Success'.

รูปที่ 10 แสดงการเก็บ Log System จากเครื่องคอมพิวเตอร์แม่ข่าย

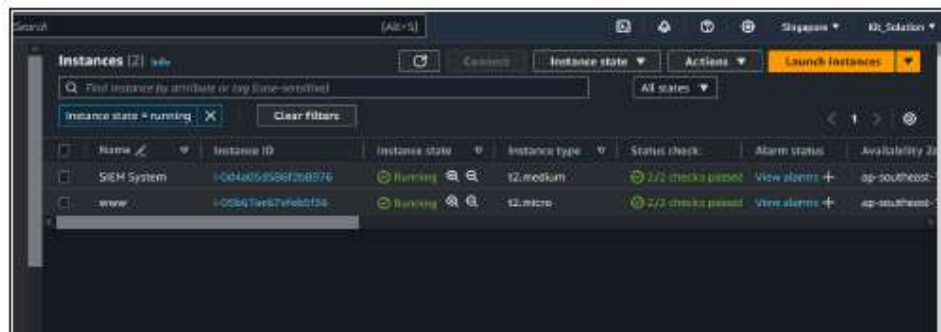
3. Application Slack สำหรับการแจ้งเตือนผ่าน Application Internet โดย Slack เป็นบริการส่งข้อความโต้ตอบแบบทันทีข้ามแพลตฟอร์มแบบฟรีบนคลาวด์ที่สร้างโดย Slack Technologies และปัจจุบันเป็นของ Salesforce แม้ว่าในตอนแรกจะได้รับการพัฒนาเพื่อการสื่อสารระดับมืออาชีพและระดับองค์กร แต่ก็ถูกนำมาใช้เป็นแพลตฟอร์มชุมชนด้วย ผู้ใช้สามารถสื่อสารผ่านการส่งข้อความถึงกัน ซึ่งผู้วิจัยได้แสดงขั้นตอนการทำงาน ดังรูปที่ 11



รูปที่ 11 แสดง Data Flow Message (Slack. Engineering, 2566)

4. ระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย CentOS7 ใช้สำหรับเว็บเซิร์ฟเวอร์ ซึ่งมีหน้าที่เป็น Honeypot โดยระบบปฏิบัติการ CentOS7 ใช้สำหรับองค์กรที่เน้นเรื่องความปลอดภัยภาพ

5. Amazon Elastic Compute Cloud (Amazon EC2) คือบริการให้เช่าระบบการประมวลผลตามความต้องการและปรับขนาดได้ใน Amazon Web Services (AWS) Cloud การใช้ Amazon EC2 ช่วยลดต้นทุนด้านฮาร์ดแวร์ สามารถพัฒนาและปรับใช้แอปพลิเคชันได้เร็วขึ้น การใช้ Amazon EC2 เพื่อเปิดใช้เซิร์ฟเวอร์เสมือนได้มากหรือน้อยตามที่ต้องการ รายละเอียดแสดงการใช้งานไว้ ดังรูปที่ 12



รูปที่ 12 แสดงแดชบอร์ดอินเทอร์เฟซผู้ใช้งานระบบ AWS

6. Kali Linux เครื่องมือทดสอบ Brute Force Attack (เดิมชื่อ Back Track Linux, 2013) เป็นระบบปฏิบัติการ Linux แบบโอเพนซอร์สที่ใช้ Debian ซึ่งมุ่งเป้าไปที่การทดสอบการเจาะข้อมูลขั้นสูงและการตรวจสอบความมั่นคงปลอดภัย การกำหนดค่า และระบบอัตโนมัติที่ช่วยให้ผู้ใช้งานมั่นใจไปทำงานที่ต้องทำให้เสร็จ Kali Linux มีการดัดแปลงเฉพาะอุตสาหกรรม รวมถึงเครื่องมือหลายร้อยรายการที่มุ่งเป้าไปที่งานด้านความมั่นคงปลอดภัยของข้อมูลต่าง ๆ เช่น การทดสอบการเจาะข้อมูล การวิจัยความมั่นคงปลอดภัย นิติคอมพิวเตอร์ วิศวกรรมย้อนกลับ และการจัดการช่องโหว่

7. แบบประเมินประสิทธิภาพที่มีต่อการทำงานของระบบติดตาม เฝ้าระวัง และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองแบบเรียลไทม์ มีลักษณะเป็นแบบมาตราส่วนประมาณค่า 5 ระดับ (Rating Scale) แบบลิเคิร์ต (Likert) [4] เกณฑ์ในการแปลความหมายของประสิทธิภาพในเชิงความถูกต้องและความเร็วในระดับต่าง ๆ ดังนี้

ค่าเฉลี่ย 4.21 – 5.00 หมายถึง มีประสิทธิภาพในระดับมากที่สุด

ค่าเฉลี่ย 3.41 – 4.20 หมายถึง มีประสิทธิภาพในระดับมาก

ค่าเฉลี่ย 2.61 – 3.40 หมายถึง มีประสิทธิภาพในระดับปานกลาง

ค่าเฉลี่ย 1.81 – 2.60 หมายถึง มีประสิทธิภาพในระดับน้อย

ค่าเฉลี่ย 1.00 – 1.80 หมายถึง มีประสิทธิภาพในระดับน้อยที่สุด

5. ผลการวิจัย

1. ผลศึกษาวิเคราะห์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับเครื่องเซิร์ฟเวอร์ คือการมีความเสี่ยงทางไซเบอร์หรือการคาดการณ์ถึงการทำให้เกิดความเสียหายอันส่งผลกระทบต่อระบบคอมพิวเตอร์ ข้อมูล และอุปกรณ์คอมพิวเตอร์ต่าง ๆ เช่น การโจมตีด้วยไวรัสคอมพิวเตอร์ การบุกรุกเครือข่ายโดยไม่ได้รับอนุญาต การขโมยข้อมูลส่วนบุคคล และการปฏิบัติการที่เกี่ยวกับความเป็นอันตรายของระบบเครือข่ายคอมพิวเตอร์ [5]

ภัยคุกคามทางไซเบอร์มีความหลากหลายและต้องการการระมัดระวังและการป้องกันที่เหมาะสมเพื่อป้องกันความเสี่ยงและการเข้าถึงข้อมูลที่ไม่เป็นไปตามกฎหมายหรือไม่ได้รับอนุญาต ภัยคุกคามทางไซเบอร์ที่พบมากที่สุดในปัจจุบันมี 7 ประเภท ดังนี้ [6]

- 1) Malware
- 2) Phishing
- 3) SQL Injection Attacks
- 4) Cross-site Scripting (XSS)
- 5) Denial of Service (DoS)
- 6) Man-in-the-Middle Attacks
- 7) Password Attacks

จากผลการศึกษาวิเคราะห์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายในองค์กรทำให้พบว่าการโจมตีแบบ Password Attacks หรือเรียกว่า Simple Brute Force Attacks เป็นการโจมตีที่พบมากที่สุด ใน 7 ประเภทที่กล่าวมาข้างต้น ทำให้ผู้วิจัยได้ทำการวิจัยเพื่อทดสอบการติดตาม เมื่อเริ่มและแจ้งเตือน และนำไปสู่ผลการพัฒนาการแจ้งเตือนเมื่อเกิดภัยคุกคามแบบ Simple Brute Force Attacks อย่างเรียลไทม์

2. ผลพัฒนาระบบการแจ้งเตือนเมื่อเกิดภัยคุกคามแบบ Simple Brute Force Attacks อย่างเรียลไทม์จะพบว่าเมื่อมีการโจมตีเกิดขึ้นระบบ SIEM จะทำการเปรียบเทียบกับ MITRE ATT&CK Framework และระบบ SIEM ก็จะทำการบันทึกระบุเทคนิคการโจมตีคือ Password Guessing, SSH ซึ่งเป็นการโจมตีแบบ Brute Force Attacks และกำหนดค่า rule.id = 5760 ดังรูปที่ 13

rule.groups	syslog, sshd, authentication.failed
rule.hipaa	104.312.b
rule.id	5760
rule.level	5
rule.mail	false
rule.mitre.id	T1110.001, T1021.004
rule.mitre.tactic	Credential Access, Lateral Movement
rule.mitre.technique	Password Guessing, SSH
rule.nist.800.53	AU.14, AC.2
rule.pci.dss	10.2.4, 10.2.5
rule.tso	006.1, 006.8, 007.2, 007.3
Timestamp	Jan 10, 2024 @ 20:56:12.018

รูปที่ 13 แสดงการโจมตีแบบ Brute Force Attack

เมื่อผู้วิจัยนำค่าของ MITRE ATT&CK ที่ระบุ rule.id = 5760 ในระบบ SIEM มากำหนดกฎเงื่อนไขใน .XML ไฟล์ที่อยู่ในส่วนของ Rule ระบบ SIEM โดยหากพบการโจมตี rule.id = 5760 จำนวน 4 ครั้งภายใน 600 วินาทีจากไอพีต้นทางเดียวกัน ให้ระบุว่าเป็น trying to Brute Force และกำหนดเป็น rule id= "100030" ดังรูปที่ 14

```
<group name="local,syslog,sshd">
  <rule id="100030" level="10" frequency="4" timeframe="600">
    <if_matched_sid>5760</if_matched_sid>
    <same_source_ip />
    <description>IP address $(srcip) trying to Brute Force.</description>
    <group>authentication_failed,gog13_7.1,</group>
  </rule>
</group>
```

รูปที่ 14 เงื่อนไขเพื่อวิเคราะห์โจมตีแบบ Brute Force Attack

12 | กฤษ ศรีเงินทิ และคณะ

ผู้วิจัยนำค่า rule.id = 100030 เป็นข้อกำหนดการแจ้งเตือนไปที่ Application Slack ดังรูปที่ 15

```
<integration>
  <name>custom-block</name>
  <hook_url>https://hooks.slack.com/services/T05QKE26JQL/D06CF8C5CR0/9Ir4j0chHydLiAqbC4V0gayH</hook_url>
  <rule_id>100030</rule_id>
  <alert_format>json</alert_format>
</integration>
```

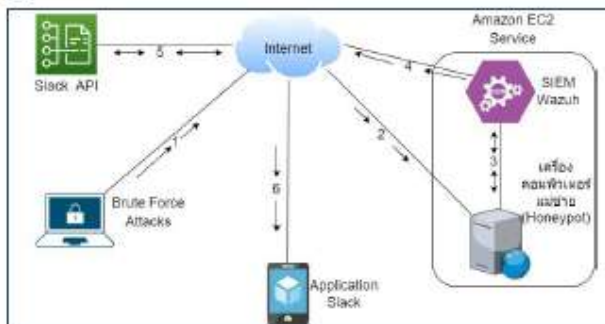
รูปที่ 15 แสดงเงื่อนไขการแจ้งเตือน Brute Force Attack

เมื่อได้ทำการโจมตีครบจำนวนตรงตามกำหนดเงื่อนไขที่ไว้แล้ว ระบบ SIEM จะทำการบันทึกการโจมตีที่เกิดขึ้นไว้ในระบบ SIEM ซึ่งจะช่วยให้ทราบว่ามีการพยายามโจมตีเครื่องคอมพิวเตอร์แม่ข่ายแบบ Simple Brute Force Attacks และแสดงหมายเลขกฎเป็น 100030 ดังรูปที่ 16

> Jan 18, 2024 @ 19:59:10.103 IP address 59.11.28.35 trying to Brute Force.	10	100030
> Jan 18, 2024 @ 19:59:10.101 sshd: authentication failed.	5	5700
> Jan 18, 2024 @ 19:59:08.367 sshd: authentication failed.	5	5700
> Jan 18, 2024 @ 19:59:06.122 sshd: authentication failed.	5	5700

รูปที่ 16 แสดงการวิเคราะห์โจมตีแบบ Brute Force Attack

ต่อมาจะส่งคำพารามิเตอร์ที่ได้เฝ้าติดตามเครื่องคอมพิวเตอร์แม่ข่าย ดังรูปที่ 13 ทั้งนี้ เมื่อระบบได้รับการวิเคราะห์ตรงตามเงื่อนไขที่ได้กำหนดค่าจะทำการแจ้งเตือนไปยัง Slack API เพื่อให้ผู้ดูแลระบบทราบถึงเหตุการณ์การโจมตีแบบสุ่มรหัสผ่าน โดยมีกระบวนการทำงานเพื่อส่งข้อความการแจ้งเตือนการโจมตีไปยังผู้ดูแลระบบ ดังรูปที่ 17



รูปที่ 17 แสดงกระบวนการทำงานการแจ้งเตือนการโจมตี

เมื่อเกิดการโจมตีเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งเป็นไปตามกฎที่กำหนดไว้ ดังรูปที่ 14 จากนั้น Elasticsearch ในระบบ Wazuh Server ก็จะนำค่า Rule ID = 100030 ที่เกิดขึ้นจากกฎ ที่กำหนดขึ้นไป เปรียบเทียบกับเงื่อนไขที่อยู่ใน Integrates ในชุดคำสั่ง .XML ของระบบ SIEM ว่ามีชื่อเงื่อนไขใดๆ ที่ตรงกับ Rule ID = 100030 หรือไม่ หากพบว่าตรงกับ Rule ID = 100030 และค่าที่กำหนดไว้นั้น ให้ทำการส่ง ข้อความไปยัง API ตามช่องทางใด และพร้อมรายละเอียดจาก Log System ที่เก็บอยู่ในรูปแบบ JSON โดย การใช้ชุดคำสั่งไพทอนเรียกค่าต้องการส่งไปยังผู้ดูแลระบบเครื่องคอมพิวเตอร์แม่ข่าย ให้ทราบถึงภัยคุกคามที่เกิดขึ้น และตรวจสอบและดำเนินการป้องกันหรือยับยั้งต่อไป ดังรูปที่ 18



รูปที่ 18 แสดงการแจ้งเตือนผ่าน Application Slack

3. ผลการประเมินประสิทธิภาพการวิเคราะห์และแจ้งเตือนภัยคุกคามทางไซเบอร์แบบเรียลไทม์ โดย นำระยะเวลาที่ใช้ในการวิเคราะห์และการแจ้งเตือนมาหาค่าเฉลี่ย ($\bar{X}$) และการทดสอบการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายและระยะที่ใช้ในการแจ้งเตือนผ่าน Application Slack เปรียบเทียบกับการโจมตีแบบ Brute Force Attack ที่ถูกบันทึกลงไปในระบบ SIEM มีดังนี้

จากการทดสอบจำนวน 5 ชุด ผลการวิเคราะห์และการแจ้งเตือนภัยคุกคามทางไซเบอร์ มีค่าเฉลี่ย ($\bar{X}$) ซึ่งอยู่ในระดับมากที่สุด ($\bar{X} = 5.00$) โดยกำหนดระยะเวลาที่ใช้ในการวิเคราะห์ที่ติดตามและระบบแจ้งเตือน ดังนี้

ระยะเวลาการวิเคราะห์หรือแจ้งเตือน	1 วินาที – 5 วินาที หมายถึงอยู่ในระดับ 5
ระยะเวลาการวิเคราะห์หรือแจ้งเตือน	6 วินาที – 10 วินาที หมายถึงอยู่ในระดับ 4
ระยะเวลาการวิเคราะห์หรือแจ้งเตือน	11 วินาที – 15 วินาที หมายถึงอยู่ในระดับ 3
ระยะเวลาการวิเคราะห์หรือแจ้งเตือน	16 วินาที – 20 วินาที หมายถึงอยู่ในระดับ 2
ระยะเวลาการวิเคราะห์หรือแจ้งเตือน	21 วินาที – 25 วินาที หมายถึงอยู่ในระดับ 1

ผลการทดสอบระบบการวิเคราะห์และการแจ้งเตือนเครื่องคอมพิวเตอร์แม่ข่าย จะพบว่าระบบ SIEM ได้ทำการวิเคราะห์และบันทึกการโจมตีที่ตรงตามเงื่อนไขกำหนด ผู้วิจัยนำเวลาเริ่มโจมตีมาเปรียบเทียบกับเวลา ที่ทำการแจ้งเตือน ซึ่งเวลาเป็นการบันทึกด้วยระบบ SIEM อัตโนมัติ รายละเอียดดังรูปที่ 19 และ 20



รูปที่ 19 แสดงผลการวิเคราะห์และบันทึกการโจมตี

previous_output	Jan 18 13:56:16 ip-172-31-45-16 sshd[7689]: Failed password for root from 58.11.28.33 port 59532 ssh2 Jan 18 13:56:16 ip-172-31-45-16 sshd[7689]: Failed password for root from 58.11.28.33 port 59532 ssh2 Jan 18 13:56:16 ip-172-31-45-16 sshd[7689]: Failed password for root from 58.11.28.33 port 59532 ssh2
rule.description	IP address 58.11.28.33 trying to Brute Force.
rule.firedtimes	6
rule.frequency	4
rule.ppg13	7.1
rule.groups	local, syslog, sshd, authentication_failed
rule.id	100030
rule.level	16
rule.mail	false
timestamp	Jan 18, 2024 @ 20:56:12.828

รูปที่ 20 แสดงรายละเอียดการวิเคราะห์และรูปแบบการโจมตี

เมื่อมีการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายที่เกิดขึ้น ตรงตามกฎที่ผู้วิจัยกำหนดไว้ ดังรูปที่ 19 และ รูปที่ 20 จะพบว่ามีการบันทึกเวลากิจกรรมที่เกิดขึ้นตามอ้างอิงจากระบบ SIEM ลงบันทึกไปใน Log System ของระบบ SIEM เพื่อเป็นการยืนยันเหตุการณ์ที่เกิดขึ้น ณ ขณะเกิดเหตุการณ์ ตั้งแต่เริ่มจนถึงจุดสิ้นสุดตรงตามกฎเงื่อนไขที่กำหนด จึงนำค่ามาคำนวณระยะเวลาที่ใช้ในการวิเคราะห์เพื่อระบุภัยคุกคามที่เกิดขึ้นกับเครื่อง

คอมพิวเตอร์แม่ข่ายและการแจ้งเตือนภัยคุกคามไปยัง Application Slack ที่ตรงตามชุดคำสั่งสอดคล้องกับเงื่อนไข ที่ผู้วิจัยได้กำหนดไว้ก่อนแล้วนั้น โดยการทดสอบเพื่อแสดงการค่าประสิทธิภาพของการวิเคราะห์ หรือแจ้งเตือน ผู้วิจัยได้ทำการทดสอบ โดยแต่ละชุดการทดสอบ แบบการเข้าใช้เครื่องคอมพิวเตอร์แม่ข่ายผ่าน SSH โดยผู้ใช้งานเป็น Root และใส่รหัสผ่านไม่ถูกต้องจำนวน 4 ครั้งต่อการทดสอบจำนวน 1 ชุด และทดสอบจำนวน 5 ชุด เพราะค่าเงื่อนไขที่กำหนดในค่า .XML เป็นค่ากำหนดเงื่อนไขคงที่ ด้วยหลักการโจมตียังคงเป็นการคาดเดารหัสผ่านช่องทาง SSH Port เมื่อนำมารวมจำนวนครั้งการคาดเดารหัสผ่านเท่ากับ 20 ครั้ง จึงเป็นการทดสอบซ้ำด้วยเงื่อนไขเดิม และไม่ได้แปรผันตามช่วงเวลาของการทดสอบแต่อย่างใด ซึ่งได้ผลการทดสอบตามรายละเอียดจากตารางที่ 1 และตารางที่ 2

ตารางที่ 1 ผลระยะเวลาการวิเคราะห์ติดตามการโจมตีแบบ Brute Force Attack

วัน	11-Apr-24	11-Apr-24	11-Apr-24	11-Apr-24	11-Apr-24			
เวลาเริ่ม	00.22.21	00.33.36	00.41.53	00.54.06	01.05.19	รวม	N	$\bar{X}$
เวลาสิ้นสุด	00.22.23	00.34.00	00.41.53	00.54.28	01.05.19			
ครั้งที่	1	2	3	4	5			
ระดับ	5	5	5	5	5			
						25	5	5.00

ผลการทดสอบตารางที่ 1 แสดงผลการตรวจจับ Rule ID = 100030 ในช่วงระยะเวลาการใส่รหัสผ่านที่ไม่ถูกต้องให้จำนวนต่างกันในการทดสอบชุดที่ 1, 2, 4 และติด ๆ กัน ชุดที่ 3, 5 นั้น เพื่อทดสอบการประมวลผลการตรวจจับที่เป็นไปตามเงื่อนไขที่ได้กำหนดไว้ในค่า .XML ไฟล์ ซึ่งถ้าหากเป็นบุคคลใส่รหัสผิดก็จะต้องมีการทบทวนรหัสผ่านก่อนที่จะใส่ในครั้งต่อไป ซึ่งต่างจากการ Brute Force Attack ที่พยายามให้เข้าเครื่องคอมพิวเตอร์แม่ข่ายให้เร็วที่สุด และใช้เวลาให้น้อยที่สุด

ตารางที่ 2 ผลระยะเวลาการแจ้งเตือนแบบเรียลไทม์

วัน	11-Apr-24	11-Apr-24	11-Apr-24	11-Apr-24	11-Apr-24			
เวลาเริ่ม	00.22.21	00.33.36	00.41.53	00.54.06	01.33.36	รวม	N	$\bar{X}$
เวลาสิ้นสุด	00.22.23	00.34.00	00.41.53	00.54.28	01.33.36			
ครั้งที่	1	2	3	4	5			
ระดับ	5	5	5	5	5			
						25	5	5.00

ผลการทดสอบตารางที่ 2 เมื่อตรวจจับ Rule ID = 100030 ในเวลาที่สิ้นสุดการ Brute Force Attack ระบบ SIEM ได้มีการแจ้งเตือนไปยังผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายผ่าน Slack Application โดยเปรียบเทียบ

16 | กฤษ ศรีเงินทิ และคณะ

ที่แสดงว่ามีกิจกรรมการตรวจจับการ Brute Force Attack โดยใช้ Rule ID = 100030 ในการส่งค่าการแจ้งเตือน โดยเปรียบเทียบกับเวลาได้ข้อความมีเวลาเดียวกันกับเมื่อ SIEM แสดง Log ที่เป็น Rule ID = 100030

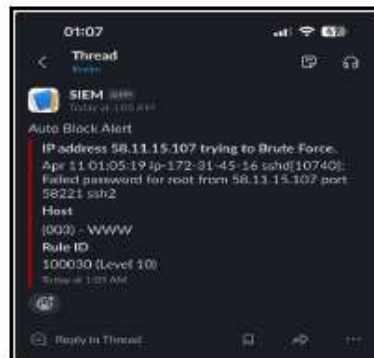
นอกจากนั้น ในรูปที่ 21-23 ยังได้แสดง Brute Force Attack แบบเว้นระยะเวลา, แบบระยะเวลาติดกันและแบบแจ้งเตือน ตามลำดับ

> Apr 11, 2024 @ 00:34:09.590 - IP address 58.11.15.107 trying to Brute Force.	10	100030
> Apr 11, 2024 @ 00:35:48.330 sshd: authentication failed.	5	1700
> Apr 11, 2024 @ 00:35:42.280 sshd: authentication failed.	5	1700
> Apr 11, 2024 @ 00:35:36.530 sshd: authentication failed.	5	1700

รูปที่ 21 แสดง Brute Force Attack แบบเว้นระยะเวลา

> Apr 11, 2024 @ 01:05:19.570 - IP address 58.11.15.107 trying to Brute Force.	10	100030
> Apr 11, 2024 @ 01:05:19.194 sshd: authentication failed.	5	1700
> Apr 11, 2024 @ 01:05:19.194 sshd: authentication failed.	5	1700
> Apr 11, 2024 @ 01:05:19.194 sshd: authentication failed.	5	1700

รูปที่ 22 แสดง Brute Force Attack แบบระยะเวลาติดกัน



รูปที่ 23 แสดงการแจ้งเตือน Brute Force Attack

6. อภิปรายผลและข้อเสนอแนะ

1. ในงานวิจัยนี้เป็นการวิเคราะห์ภัยคุกคามที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งผู้วิจัยได้ทำการจัดเก็บ Log System จากเครื่องคอมพิวเตอร์แม่ข่ายที่เป็นเหยื่อล่อ นำมาวิเคราะห์การโจมตี และกำหนดกฎเงื่อนไขเพิ่มเติม เพื่อใช้ในการติดตาม ฝ้าระวัง และแจ้งเตือน ภัยคุกคามแบบ Brute Force โดยเมื่อเกิด

เหตุการณ์ภัยคุกคามที่เครื่องคอมพิวเตอร์แม่ข่ายตรงกับคำพารามิเตอร์ที่กำหนดไว้ ก็จะทำให้ทราบถึงภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายได้โดยง่าย เพราะเทคนิคการโจมตีทางไซเบอร์ได้มีการตั้งค่าเงื่อนไขพร้อมการแจ้งเตือนไปยังผู้ดูแลระบบเครื่องคอมพิวเตอร์แม่ข่าย และยังสามารถส่งข้อมูลที่จำเป็นใช้ในการแจ้งเตือนไปได้ภายในครั้งเดียว และลดระยะเวลาของการตรวจสอบเครื่องคอมพิวเตอร์แม่ข่ายไปพร้อม ๆ กันได้

2. การแจ้งเตือนเมื่อเกิดภัยคุกคามแบบ Brute Force Attacks อย่างเรียลไทม์นั้น ผู้วิจัยได้ให้ความสำคัญเรื่องเวลาการแจ้งเตือนให้กับผู้ดูแลระบบ เพราะหากระบบ SIEM ยังแจ้งเหตุภัยคุกคามทางไซเบอร์ได้ใกล้เคียงกับเวลาจริงหรือเรียลไทม์มากเท่าใดก็จะยิ่งเพิ่มประสิทธิภาพในการป้องกันภัยคุกคามทางไซเบอร์ได้มากเท่านั้น จากงานวิจัยของ Abdullah Almurayh และ Nasro Min-Allah [7] ที่ได้มีการศึกษาเกี่ยวกับ Password Cracking with Brute Force Algorithm and Dictionary Attack Using Parallel Programming โดยพบว่าสามารถลดอัตราที่สับสนผ่านด้วยความเร็วเป็น 11.5 เท่า และ 10.4 เท่าสำหรับรหัสผ่านที่มีและไม่มีอักขระพิเศษ ตามลำดับ และ brute force สามารถเร่งความเร็วได้ 4.4 เท่า

3. การประเมินประสิทธิภาพการวิเคราะห์และแจ้งเตือนภัยคุกคามแบบเรียลไทม์ ซึ่งงานวิจัยนี้ได้สะท้อนผลการเปรียบเทียบระยะเวลาการแจ้งเตือนกับการบันทึกข้อมูลภัยคุกคามที่เกิดขึ้น จะมีค่าระยะเวลาตามผลการวิเคราะห์ภัยคุกคามทางไซเบอร์ได้ผลค่าประสิทธิภาพในระดับมากที่สุด ($\bar{X} = 5.00$) และค่าการแจ้งเตือนมีค่าประสิทธิภาพอยู่ในระดับมากที่สุด ($\bar{X} = 5.00$) เช่นกัน ซึ่งเป็นผลดีในการนำเอาระบบนี้ไปใช้งานจริง หากเกิดภัยคุกคามทางไซเบอร์ตามที่ได้กำหนดการเฝ้าระวังไว้ อย่างไรก็ตาม ค่าความรวดเร็วนี้อาจจะต้องอาศัยประสิทธิภาพของระบบเครือข่ายคอมพิวเตอร์หรืออินเทอร์เน็ตที่องค์กรเชื่อมต่ออยู่ด้วย นอกจากนั้น การแจ้งเตือนไปยัง Application Slack นั้น ยังไม่มีค่าใช้จ่ายใด ๆ สำหรับการเรียกใช้งาน ผ่าน API และใช้งานได้ทั้งบนเครื่องโมบายล์ และคอมพิวเตอร์ส่วนบุคคล ซึ่งเป็นการเพิ่มความสะดวกและคล่องตัวให้กับผู้ดูแลระบบเครื่องคอมพิวเตอร์แม่ข่ายให้ติดตาม เฝ้าระวังการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายได้ตลอดเวลา ในทุกที่ ๆ สามารถเข้าถึงอินเทอร์เน็ต หากแม้ว่าไม่ได้อยู่กับเครื่องคอมพิวเตอร์แม่ข่ายนั้น ๆ อีกทั้งยังประหยัดค่าใช้จ่ายในการพัฒนาแอปพลิเคชันเพื่อใช้สำหรับการแจ้งเตือนอีกด้วย

อย่างไรก็ตาม การศึกษาวิจัย การพัฒนาระบบติดตาม เฝ้าระวัง และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองแบบเรียลไทม์ ผู้วิจัยมีข้อเสนอแนะจากการศึกษาค้นคว้าดังนี้

1. ข้อเสนอแนะในการนำผลการวิจัยไปใช้งานจริง ซึ่งจากระบบที่ได้มีการพัฒนาขึ้นนี้ สามารถนำไปปรับใช้กับองค์กรที่ต้องการรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการแบบเข้าถึงจากภายนอกองค์กรให้มีการแจ้งเตือนภัยคุกคามทางไซเบอร์ไปยังผู้ดูแลระบบอันเป็นการยับยั้งการโจมตีทางไซเบอร์ได้ อีกทั้งเหมือนเป็นการพัฒนาระบบแบบโอเพนซอร์ส (Open Source) ที่ไม่ได้มีค่าใช้จ่ายใด ๆ ในด้านค่าลิขสิทธิ์ (License) ยิ่งทำให้นำไปใช้ได้อย่างง่าย หากองค์กรนั้น ๆ มีข้อจำกัดด้านงบประมาณสำหรับการ

รักษาความมั่นคงปลอดภัยไซเบอร์ เช่น สถาบันการศึกษา วิสาหกิจขนาดกลางและขนาดย่อม (SME) องค์กรไม่หวังผลกำไรต่าง ๆ และหน่วยงานภาครัฐ

2. ข้อเสนอแนะในการวิจัยครั้งต่อไป จากการวิจัยนี้ยังคงเป็นการวิจัยการโจมตีทางไซเบอร์แบบ Brute Force Attack เพียงอย่างเดียวจะนำระบบ SIEM [8] นี้ไปพัฒนาต่อเรื่องการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายในแบบอื่น เช่น การโจมตีด้วย แรนซัมแวร์ มัลแวร์ การโจมตีแบบ DDoS เนื่องจากการทำงานของระบบ SIEM จะอ่านข้อมูลจาก Log System ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่าย หากระบบ SIEM อ่านค่ากิจกรรมที่เกิดขึ้นอันเป็นผลที่น่าสงสัยหรือไม่ปกติ ก็สามารถให้ AI ให้ช่วยในการวิเคราะห์ข้อมูลที่ส่งออกจากระบบ SIEM เพื่อช่วยในการวิเคราะห์การโจมตี รวมทั้งแนวทางการแก้ไข ยับยั้ง หรือการกู้คืนสภาพ ของระบบได้

7. เอกสารอ้างอิง

- [1] สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2566). ข้อมูลเชิงสถิติการให้บริการ. จาก <https://www.ncsa.or.th/service-statistics.html>.
- [2] ATT&CK M. (2023). Versions of ATT&CK. จาก <https://attack.mitre.org/resources/versions>.
- [3] Zhang, S., Xie, X., and Xu Y. (2020). A Brute-Force Black-Box Method to Attack Machine Learning-Based Systems in Cybersecurity. IEEE Access, 8.
- [4] สุบิน ยุระรัช. (2565). ทำไมต้องลิเคิร์ด?. วารสารนวัตกรรมและการจัดการศูนย์ส่งเสริมและพัฒนางานวิจัย มหาวิทยาลัยศรีปทุม.
- [5] ประเมศวร์ กุमारบุญ. (2561). การส่งเสริมการศึกษาในวิชาอาชญกรรมไซเบอร์. กรุงเทพฯ: วารสารวิชาการอาชีวศึกษาและนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ.
- [6] บริษัท ไซเบอร์ อีลีท จำกัด. (2566). 7 ประเภท ของภัยคุกคามทางไซเบอร์ที่พบบ่อย. จาก <https://www.cyberelite.co.th>.
- [7] Abdullah Almurayh and Nasro Min-Allah. (2023). Password Cracking with Brute Force Algorithm and Dictionary Attack Using Parallel Programming. Applied Sciences-Vol. 13. Iss: 10, pp5979-5979.
- [8] Filkins B. (2019). An Evaluator's Guide to NextGen SIEM. SANS Institute.
- [9] วรัช พงษ์ชนนี. (2562). ระบบเฝ้าระวังและตรวจจับภัยคุกคามเว็บ เซิร์ฟเวอร์ Mini SOC Web Server. กรุงเทพฯ: มหาวิทยาลัยเทคโนโลยีมหานคร.
- [10] กิตติภณ พละการ, กิตติภพ พละการ, สมชาย ประสิทธิ์จตุระกุล และ สุกรี สินธุภิญโญ. (2561) Python ๑๐๑. พิมพ์ครั้งที่ 2. กรุงเทพฯ: คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.
- [11] Vlad-Mihai C. (2016). SIEM (Security Information and Event Management Solutions) Implementation in Private or Public Clouds. Scientific Bulletin of Naval Academy.

www.ijert.org



IJERT

International Journal of Engineering Research & Technology
ISSN : 2278-0181
www.ijert.org

Provisional Acceptance Letter

Dear Kit Sringendee,

Thank you for your contribution in our journal. At the same time we gladly inform you that your submitted paper, for which you are the correspondence author, has been passed through our initial screening stage and is accepted for further publication process in IJERT.

As a result, your paper will publish in the **Volume 13 , Issue 06 , June - 2024 of IJERT** according to the further review process & priorities.

Your Manuscript details are as follow:

Paper Title : Developing Proactive Cyber Threat Defense Systems on Server Computers Using Honeypot Techniques
Paper Id : IJERTV13IS060012

Your Paper will publish in online & print version, after once you finish **simple 3 Step registration process.**

Please Log in to your online IJERT-EMS author manger account, **for detailed registration procedure.**

Looking forward to a good collaboration,



Thanking You,

Yours Faithfully,

Editor, IJERT

www.ijert.org

Developing Proactive Cyber Threat Defense Systems on Server Computers Using Honeypot Techniques

Kit Sringendee, Prasong Praneetpolgrang, Surasak Mungsing

Information Technology Program
 Faculty of Information Technology
 Sripatum University, Bangkok, Thailand

Abstract— This research focuses on proactive cyber threat prevention on server computers using honeypot and bait techniques. The objective is to anticipate and intercept unauthorized attempts to guess usernames or passwords to gain access to the server computers. In this study, honeypots and bait techniques were used to simulate the services of an organization's server computer, which can be accessed from any public network. The developed system collects data on activities and events from these honeypots mechanisms, analyzes this data, and generates protective conditions based on the findings. These conditions are then compared with newly defined parameters. When the system detects a match with these predefined conditions, it immediately acts to prevent cyber threats to the server computer. The primary goal is to halt ongoing cyber attacks on the server computers and continuously monitor and manage the server computers in case of repeated cyber intrusions.

Keywords— Honeypot, Analyzes, Server

I. INTRODUCTION

Currently, Security Information and Event Management (SIEM) systems are utilized to address cybersecurity issues by collecting event data from various sources and analyzing it to detect abnormal activities. Integrating SIEM with honeypot techniques is particularly intriguing. Additionally, studying attacks on Honeypots helps system administrators understand these attacks and develop further defenses. According to the research by Anil Tom and MN Nachappa [1], honeypots are crucial for detecting and analyzing malicious network traffic. Implementing SIEM enhances the monitoring, analysis, and alerting of threats to organizational server computers.

Given the issues, the researcher has devised new methods to protect against potential Brute-Force Attacks on the server. This research focuses on the SIEM and details as follow:

1. Analyze cyber threats on server computers using honeypots.
2. Develop a system to prevent Brute Force Attacks on server computers.
3. Evaluate the effectiveness of the cyber threat prevention system against Brute Force Attacks.

II. MOTIVATION

Implementation of Security Information and Event Management Systems.

The use of Security Information and Event Management systems involves the installation of both a central server and monitoring servers. This comprehensive setup allows for detailed system log inspection to identify activities on servers providing internet services. When anomalies meeting predefined criteria are detected, the SIEM system, following administrator-defined commands, initiates actions on the relevant servers.

To facilitate immediate response, the SIEM system utilizes an Application Programming Interface (API) to send commands to servers equipped with pre-configured command programs. Subsequent actions are meticulously monitored through system logs to ensure rapid and accurate responses to potential security threats. This integration creates a dynamic and automated security infrastructure, enhancing the resilience and overall responsiveness of the server systems.

III. METHODOLOGY

A. Literature Review of Relevant Concepts and Theories

1. Operation of SIEM in receiving Log System data from the server.
2. Storing Log System data generated by Honeypots [2] to capture threat activities on the server.
3. Reading Log System data written in JSON format to identify the generated rule.id and MITRE ATT&CK values [3] to detail the nature of the attacks.

The SIEM system [4] utilized by the researcher to detect Brute-Force Attack cyber threats is an open-source solution called Wazuh [5]. The Wazuh Server operates in conjunction with the Elastic Stack [6]. When an event occurs on a server computer, the Agent program (beats) installed on the server computer copies the Log System data and sends it to the SIEM. The data is processed in Logstash and then stored in Elasticsearch [7] in JSON format. The system compares the obtained Log values with the rule.id values configured in the SIEM to match the events with specific rule.ids. Fig. 1.

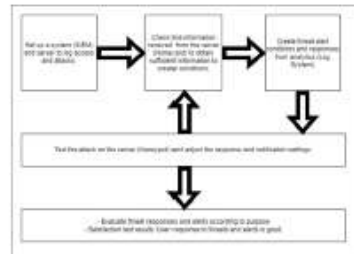


Fig. 1. Research Conceptual Framework

The SIEM system, as described above, allows the Log System on the server computer with the installed Agent to receive various commands. These commands can direct actions such as protecting the server computer or executing specified instructions.

The researcher installed an Agent to collect Log System data from the server computer used as a Honeypot, allowing access from public networks or the internet. This research, the installation was performed on AWS Cloud Services.



Fig. 2. Log System from Honeypot

Fig. 2 illustrates the log data stored during the period from March 16th, 2024 at 00:00 hours to April 15th, 2024 at 23:30 hours. It can be observed that there was a total of 35,968 log entries during this timeframe. Upon analysis by the researchers, it was found that the attacks primarily consisted of SSH Access attempts using the username "Root," corresponding to rule.id = 5760, as depicted in Fig. 3.

rule.id	5760
rule.level	1
rule.enabled	True
rule.action.id	1110, 1101, 1102, 1103
rule.action.description	Credential Access, Lateral Movement
rule.action.category	Password Guessing, SSH
rule.source.ip	10.10.10.1, 10.10.10.2
rule.target.ip	10.10.10.1, 10.10.10.2
rule.target.port	22, 22, 22, 22, 22, 22
timestamp	Apr 11, 2024 4 13:03:00 AM

Fig. 3. rule.id 5760 is Credential Access

By selecting only, the entries with rule.id = 5760, which represents attempts to access the network computer via SSH with incorrect passwords, it was found that there were a significant number of occurrences, totaling 3,287 instances. This indicates a notable attempt at Brute Force Attack.

Hence, the value of rule.id 5760 was utilized to establish new conditions for preventing such attacks on the network computer. It can be observed that there were attempts to access the network computer via SSH, as indicated by the MITRE ATT&CK technique, and confirmed by the rule.id value of 5760. This ID can be utilized to formulate conditions within the rule set of the SIEM.

B. Utilizing Log System from Honeypot to Establish Conditions and Test Protection Mechanisms

1. Creating a new rule.id in the SIEM system in .xml file. Develop a new rule.id within the SIEM system's rules using an .xml file. This rule should employ the MITRE ATT&CK framework and trigger when the cumulative count exceeds four occurrences, thereby initiating a defense mechanism against Brute Force attacks.

2. Testing the new rule.id condition created in the .xml file. The new rule.id should be tested against an SSH Brute Force attack. If an IP address attempts to randomly guess passwords four times within a 10-minute interval, the system should immediately block that IP address.

3. Setting drop packet Intervals in SIEM parameters. Configure the system to drop packets at specified intervals according to the SIEM system parameters. When researchers obtain data from Step 1, it becomes evident that incorporating rule.id 5760 as a new condition ensures that repeated SSH Brute Force attacks, reaching four attempts within 600 seconds, will be logged in the SIEM system as rule id = 100030.

The intrusion detection system was tested using the Nmap program, a programmatic scanning tool, to assess its ability to detect brute force attacks attempting to gain unauthorized access to the network computer via SSH. Nmap was employed to conduct password guessing attacks, simulating a brute force attack scenario. This testing of the intrusion detection system's effectiveness serves to ensure the security of the network computer before deploying it into a public network environment.

rule.id	100030
rule.level	1
rule.enabled	True
rule.action.id	1110, 1101, 1102, 1103
rule.action.description	Credential Access, Lateral Movement
rule.action.category	Password Guessing, SSH
rule.source.ip	10.10.10.1, 10.10.10.2
rule.target.ip	10.10.10.1, 10.10.10.2
rule.target.port	22, 22, 22, 22, 22, 22
timestamp	Apr 11, 2024 4 13:03:00 AM

Fig. 4. Log detail rule id 100030 in SIEM

Implementation and Testing of the System in a Real-World Scenario. Fig. 4, it is observed that there were attempts to access the server via SSH [8], as defined by the set conditions. The researchers utilized these parameters to prevent SSH Brute Force attacks. By configuring rule.id in the SIEM system, the researchers established conditions that log rule.id 100030 when such attempts occur.

Having successfully recorded and displayed rule.id 100030 in the SIEM, the researchers designed a process where the

SIEM sends commands to protect the main server through an installed agent, as demonstrated in Fig. 5.

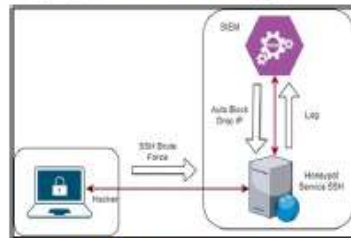


Fig. 5. Flow System Diagram

C. Evaluation of the Effectiveness of Cyber Attack

Prevention on Main Server Against Brute Force Attacks

The effectiveness of the cyber-attack prevention system against Brute Force Attacks on server was evaluated using an event response analysis technique based on predefined conditions. This evaluation employed a 5-level (Likert) [9] rating scale to interpret the effectiveness in terms of accuracy and speed, as follows level of effectiveness.

- A score of 4.21 – 5.00 indicates the highest.
- A score of 3.41 – 4.20 indicates a high.
- A score of 2.61 – 3.40 indicates a moderate.
- A score of 1.81 – 2.60 indicates a low.
- A score of 1.00 – 1.80 indicates the lowest.

IV. RESEARCH RESULTS

A. Results of Cyber Threat Analysis on Honeypot Server

The analysis of cyber threats on honeypot servers [10] reveals various forms of insights:

- **Attack Patterns**
The analysis of threats on honeypots enables administrators to understand common attack patterns, which can directly aid in preventing attacks on operational systems.
- **Attacker Types**
Threat analysis also helps identify the types of attackers targeting honeypot servers. This understanding is crucial for developing appropriate counter-strategies and defenses.
- **Vulnerabilities and Risks**
Through threat analysis, vulnerabilities and risks that honeypot servers might have can be identified. This information is instrumental in enhancing the security of operational systems.
- **Attack Data and Techniques**
Managing the data and techniques gleaned from threats can be used to train and improve the skills and understanding of involved personnel, such as system administrators and software developers.
Honeypots are used to gather information about potential attackers and serve as valuable tools in bolstering the security of computer systems. They allow administrators to understand and effectively respond to attacks. Research by Stefan Machmeier [11] highlights that honeypots are employed to

collect data on attackers by simulating vulnerable targets in cloud environments, aiming to improve security infrastructure.

B. Results of Developing a Cyber Threat Prevention System on Main Server Computers Against Brute Force Attacks Using Event Response Analysis Techniques

The development of a cyber threat prevention system on server [12] against Brute Force Attacks using predefined event response analysis techniques reveals that when an attack occurs, the SIEM compares it with the MITRE ATT&CK Framework. The SIEM then records and identifies the attack technique as Password Guessing [13], SSH, which constitutes a Brute Force Attack, and assigns it rule.id = 5760 as shown in Fig. 6.

rule.id	5760
rule.level	5
rule.name	False
rule.mitre.id	T1110.001, T1021.004
rule.mitre.tactic	Credential Access, Lateral Movement
rule.mitre.technique	Password Guessing, SSH
rule.mitre.sub_id	60.14, 60.7
rule.mitre.sub	60.2.4, 60.2.5
rule.mitre	60.1, 60.8, 60.2, 60.3
timestamp	Apr 21, 2024 @ 18:16:54.779

Fig. 6. Detail rule.id 5760

When researchers applied the MITRE ATT&CK values indicating rule.id = 5760 in the SIEM to define rules in the XML file format within the Rule section of the SIEM, the following procedure was established.

If rule.id = 5760 is detected four times within 600 seconds from the same source IP, it should be identified as "trying to Brute Force" and assigned rule id = "100030" as illustrated in Fig. 7. This rule is then recorded in the SIEM to serve as a trigger for responding to the main server when this condition arises.

```

<group name="local,syslog,sshd">
  <rule id="100030" level="10" frequency="4" timeframe="600">
    <if matched sid=5760/>
      <name source_ip />
      <description>IP address $(srcip) trying to Brute Force.</description>
      <group authentication_failed,gg13.1.1,</group>
    </rule>
  </group>

```

Fig. 7. Conditions for analyzing Brute Force Attack

Researchers utilized the value rule.id = 100030 as a condition in configuring the parameters for response in the Configuration section of the SIEM. This configuration aims to execute commands located within the Active-response section of the SIEM.

Specifically, under the name "firewall-drop" the server computer is instructed to block packets from the IP addresses falling under the condition of rule.id = 100030 for a specified duration of 30 minutes, as detailed in Fig. 8.

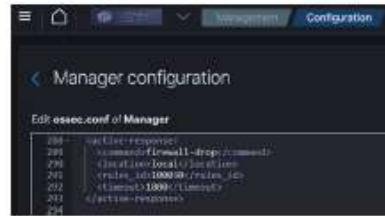


Fig. 8. Conditions for Response Brute Force Attack

Following the process, when the testing for attacks reaches the predefined conditions, the SIEM records the attacks in its log. This logging mechanism enables the SIEM to notify administrators of attempted Brute Force Attacks on the main server computer, displaying rule number 100030, as depicted in Fig. 9.

Time	Rule description	Severity	Rule ID
Apr 27, 2024 11:40:58 AM	Alert Elided by SIEM: Drop Active Response	5	100030
Apr 27, 2024 11:40:58 AM	IP address 40.203.107.146 blocking to Brute Force	10	100030
Apr 27, 2024 11:40:58 AM	rule: authentication failed	5	100030
Apr 27, 2024 11:40:58 AM	rule: authentication failed	5	100030
Apr 27, 2024 11:40:58 AM	rule: authentication failed	5	100030

Fig. 9. Log brute force attack and block IP

The blocking of the IP address originates from the public IP attempting a Brute Force Attack on the main server, which acts as a honeypot for testing attack prevention. Researchers implemented attack prevention by blocking the IP address of the attacker, preventing access to the main server computer. Upon detection of the Brute Force Attack, the SIEM sends commands to the honeypot to suspend access to the main server computer on the network. The IP address from the public IP source is blocked for a period of 30 minutes, as specified for testing attack prevention measures and to demonstrate the effectiveness of the predefined conditions, as shown in Fig. 10.

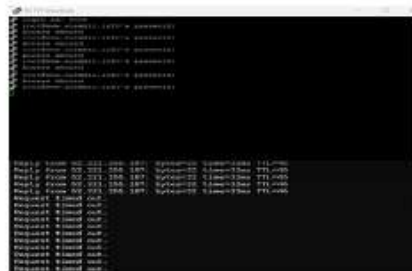


Fig. 10. Active response block IP

C. Evaluate the effectiveness of cyber threat prevention

The server acting as a honeypot against Brute Force Attacks, analysis, and notification performance were measured and compared with the detection conditions for Brute Force Attacks recorded in the SIEM. The results are as follows. The testing for attacks was divided into 5 sets. In each testing set, attempts to access the server via SSH were made 4 times or more. The analysis of the log recordings with rule.id = 100030 and the effectiveness of prevention measures were observed. The average performance was found to be at the highest level ($\bar{x} = 5.00$) when analyzing Brute Force Attacks and implementing prevention measures by dropping IP addresses, as follows:

- Number of attempts: 4 or more.
- Detection condition: rule.id = 100030.
- Prevention measure: Drop IP.

These conditions resulted in the highest average effectiveness level, demonstrating optimal performance in detecting and preventing Brute Force Attacks. The analysis and prevention effectiveness based on failed login attempts are categorized as follows:

- After 4 failed login attempts are level 5.
- After 5 failed login attempts are level 4.
- After 6 failed login attempts are level 3.
- After 7 failed login attempts are level 2.
- After 8 failed login attempts are level 1.

These ratings reflect the system's efficiency in detecting and responding to Brute Force Attacks, with the highest effectiveness achieved when responses were triggered after 4 failed login attempts.

Table I Attack protection test results Brute Force Attack Levels.

Test No.	Analysis	Drop IP	$\bar{x}$
No.1	5	5	5
No.2	5	5	5
No.3	4	4	4
No.4	5	5	5
No.5	5	5	5

Table 1 presents the test results showing the effectiveness of attack analysis and prevention. The researchers tested the prevention measures based on the log condition rule.id 100030 by simulating access to the main server computer via SSH, where the user is Root and enters an incorrect password four times. This scenario meets the set rule condition and constitutes one test set. A total of 5 test sets were conducted. The test results are detailed in Table 1. Across the 5 test sets, the analysis of log records with rule.id = 100030 and the prevention measures showed an average effectiveness at the highest level ($\bar{x} = 5.00$). This was determined by the time taken to analyze the Brute Force Attack and display the values in the SIEM system's event log Fig. 11.



Fig. 11. Log Recording

V. CONCLUSION

This research analyzes threats to main server computers using a SIEM [14], [15], [16], which can store log data from honeypot server computers. The logs generated from various events are analyzed using rule.id 100030 to understand the attacks and to establish additional rules and conditions. These rules can then be used to automate the prevention of Brute Force Attacks. When a threat event matches the predefined parameters on the main server computer, the system can be further developed to enhance cyber threat prevention efficiently. This approach also serves as a testing mechanism for main server protection before deployment in real-world scenarios.

The researchers analyzed threats to the server computer by storing log data and defining additional conditions to monitor Brute Force Attacks. When threat events match the predefined parameters, the system can effectively detect and prevent attacks. This enhances the efficiency of cyber threat prevention, aligning with the findings of Abdullah Almurayh [17], who studied password cracking using Brute Force and Dictionary Attack algorithms. They found that Brute Force attacks can be sped up by 4.4 times. Using a SIEM for real-time or near-real-time server protection significantly enhances the effectiveness of cyber threat prevention and ensures readiness to counter threats at any time.

VI. FUTURE RESEARCH

This research focuses on the development of a proactive cyber threat prevention system for network computers by employing raps and bait techniques.

A. Implementation Recommendations for Practical Application

Utilize the research outcomes for practical application to uphold the cybersecurity of network computers providing external access within organizations, which remains crucial for institutions such as educational establishments, small and medium-sized enterprises (SMEs), and governmental agencies. Despite budget constraints in cybersecurity maintenance, particularly for open-source solutions devoid of licensing costs, the ease of implementation and absence of financial limitations render them advantageous for organizations operating under budgetary constraints.

B. Future Research Considerations

Future research should consider the use of Security Information and Event Management (SIEM). Relying solely on SIEM for detecting and preventing Brute Force Attacks may be insufficient. However, SIEM can be further

developed to protect against other types of server attacks, such as ransomware, malware, or Distributed Denial of Service (DDoS) attacks. SIEM can read data from log systems and detect activities on the server computer. If suspicious or abnormal activities are detected, artificial intelligence technology can be employed to analyze the data from the SIEM. This can aid in the detection and prevention of attacks by providing recommendations for mitigation, containment, or system recovery.

REFERENCES

- [1] A. Tom and M. N. Nachappa, "A Study on Honeypots and Deceiving Attackers using Modern Honeypot Network," *International Journal of Trend in Scientific Research and Development (IJTSRD)*, vol. 5, no. 1, Nov.-Dec. 2020.
- [2] S. Bhanu, G. Khuluri, and V. Kumar, "Analysis of SSH attacks of Darknet using Honeypots," *International Journal of Engineering Development and Research*, 2013.
- [3] ATT&CK M., "Versions of ATT&CK," 2023. [Online]. Available: <https://attack.mitre.org/resources/versions/>. [Accessed: Oct. 16, 2023].
- [4] A. Tariq, J. Manzoor, M. Aziz, Z. U. A. Tariq, and A. Masood, "Open source SIEM solutions for an enterprise," *Information & Computer Security*, vol. 31, no. 1, pp. 88-107, 2022.
- [5] T. Suryantoro, B. Purnomosidi, and W. Andriyani, "The Analysis of Attacks Against Port 80 Webserver with SIEM Wazuh Using Detection and OSCAR Methods," in *Proc. 2022 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITIS)*, Dec. 2022, pp. 8-9.
- [6] C. Yu, K. Congwang, L. Jian, W. Huimei, and X. Ming, "A network attack detection system of OpenStack cloud platform based on Elastic Stack," *Proc. SPIE 12172, International Conference on Electronic Information Engineering and Computer Communication EIECC 2021*, Dec. 2021.
- [7] Yudhistira, A., & Fitriisa, Y., "Monitoring Log Server dengan Elasticsearch Logstash dan Kibana (ELK)," *RABIT: Jurnal Teknologi dan Sistem Informasi Univrab*, 8(1), 124-134, 2023.
- [8] Z. P. Chen and T. M. Khan, "Analysis of SSH Honeypot Effectiveness," *Advances in Information and Communication, Proc. 2023 Future of Information and Communication Conference (FICC)*, vol. 2, pp. 759-782, 2023.
- [9] S. Yurat, "Why Likert," *Journal of Innovation and Management, Research Promotion and Development Center, Sripartum University*, 2022. (in Thai)
- [10] D. Zielinski and H. A. Kholidy, "An Analysis of Honeypots and their Impact as a Cyber Deception Tactic," *State University of New York (SUNY) Polytechnic Institute, College of Engineering, Network and Computer Security Department, Utica, NY, USA*, Dec. 30, 2022.
- [11] Machmeier, S., "Honeypot Implementation in a Cloud Environment," *Faculty of Mathematics and Computer Science, Heidelberg University*, 2023.
- [12] D. P. Zegzhda, D. S. Lavrova, E. Pavlenko, and A. A. Shyrykina, "Cyber Attack Prevention Based on Evolutionary Cybernetics Approach," *Symmetry*, vol. 12, no. 11, p. 1931, Nov. 2020.
- [13] C. Liu, G. D. Clark, and J. Lindqvist, "Guessing Attacks on User-Generated Gesture Passwords," *Rutgers University*, vol. 1, no. 1, pp. 3, Mar. 2017.
- [14] V.-M. C., "SIEM, Security Information and Event Management Solutions Implementation in Private or Public Clouds," *Scientific Bulletin of Naval Academy*, 2016.
- [15] B. Filkins, "An Evaluator's Guide to NextGen SIEM," *SANS Institute*, 2019.
- [16] G. Granadillo, S. Gonzalez-Zarzosa, and R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructure," *Sensors*, vol. 21, no. 14, pp. 4759, 2021.
- [17] A. Almurayh and N. Min-Allah, "Password Cracking with Brute Force Algorithm and Dictionary Attack Using Parallel Programming," *Applied Sciences*, vol. 13, no. 10, pp. 5979-5979, 2023.

ภาคผนวก ง

แบบประเมินความเหมาะสมของ

Proposed Zero Trust Security Architecture แบบใหม่



แบบประเมินความเหมาะสมของ Proposed Zero Trust Security Architecture แบบใหม่

คำชี้แจง

แบบประเมินนี้ได้จัดทำขึ้นเพื่อสอบถามความคิดเห็นของผู้ทรงคุณวุฒิเกี่ยวกับ ความเหมาะสมและการยอมรับของ Proposed Zero Trust Security Architecture แบบใหม่ ซึ่งเป็นส่วนหนึ่งของการวิจัยในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

ผู้วิจัยจึงใคร่ขอความร่วมมือให้ท่านผู้ทรงคุณวุฒิตอบแบบสอบถามทุกข้อด้วยตัวของท่านเอง โดยให้ข้อมูลหรือแสดงความคิดเห็นที่ตรงกับความเป็นจริง ความรู้สึก หรือความคิดเห็นของท่านมากที่สุด ข้อมูลที่ได้จะนำไปใช้ประกอบการศึกษาและจะใช้เพื่อประโยชน์ทางวิชาการเท่านั้น ผู้วิจัยขอรับรองว่าจะไม่มีผลกระทบหรือก่อให้เกิดความเสียหายต่อตัวท่านแต่ประการใด ข้อคำถามในแบบสอบถาม แบ่งออกเป็น 3 ส่วน คือ

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ทรงคุณวุฒิ

ส่วนที่ 2 ระดับความคิดเห็นโดยรวมของผู้ทรงคุณวุฒิที่มีต่อ Proposed Zero Trust Security Architecture แบบใหม่ สำหรับองค์กร ตามแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมกับองค์กร ภายใต้งานความคิดที่ไม่ไว้วางใจใคร หากแต่ต้องตรวจสอบอยู่เสมอ

ส่วนที่ 3 ความเหมาะสมและการยอมรับของ Proposed Zero Trust Security Architecture แบบใหม่

ผู้วิจัย ขอขอบพระคุณเป็นอย่างสูงในความร่วมมือด้วยดีของท่านมา ณ โอกาสนี้

นายกฤษ ศรีเงินดี, e-mail: kit.sringendee@gmail.com, โทรศัพท์: 081-626-1475
 นักศึกษาหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
 มหาวิทยาลัยศรีปทุม

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ทรงคุณวุฒิ

1. ชื่อ-นามสกุล

.....

2. ตำแหน่งงานของท่าน (โปรดระบุ)

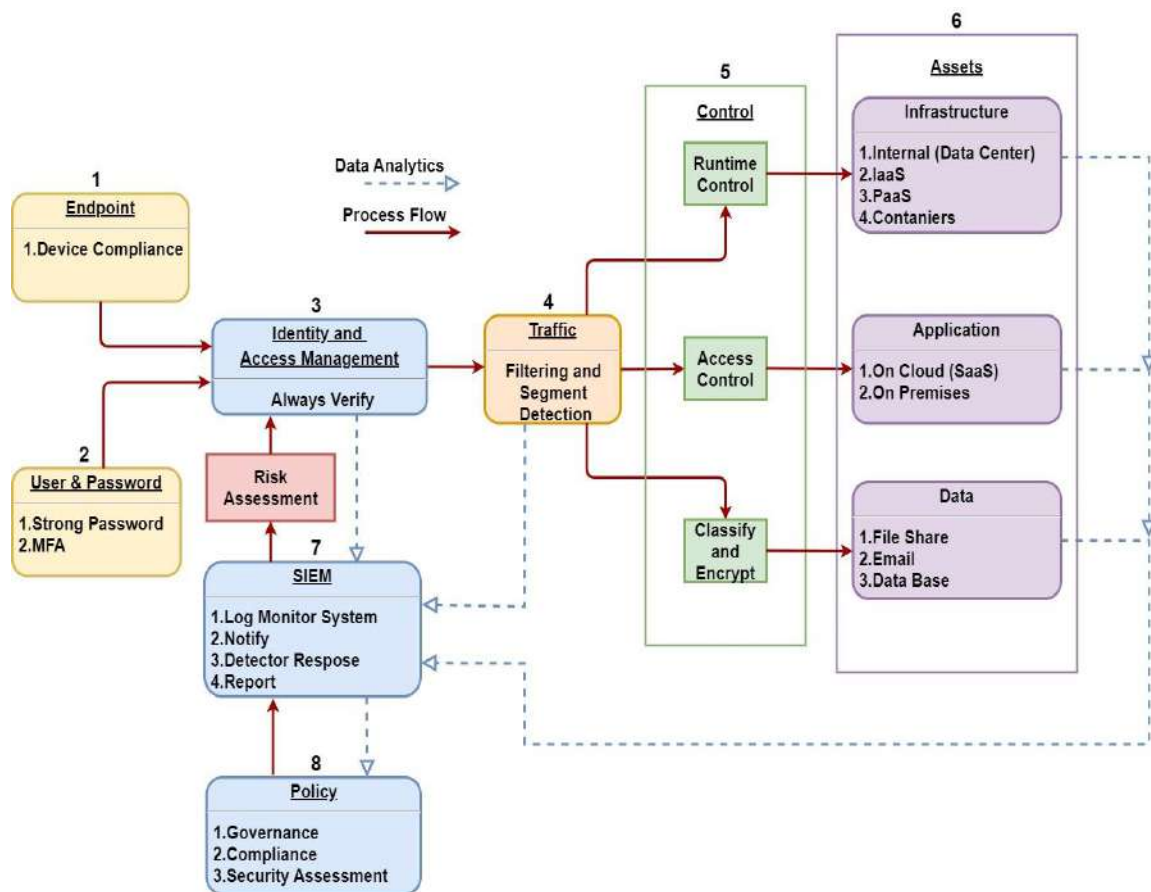
.....

3. ระยะเวลาของประสบการณ์ที่ท่านได้ทำงานด้านเทคโนโลยีดิจิทัล

- ☐ น้อยกว่า 3 ปี ☐ 3-5 ปี
☐ 6-10 ปี ☐ มากกว่า 10 ปี

**ส่วนที่ 2 ความเหมาะสมและการยอมรับของ Proposed Zero Trust Security Architecture แบบใหม่
 สำหรับองค์กร ตามแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ที่
 เหมาะสมกับองค์กร ภายใต้อาณัติความคิดที่ไม่ไว้วางใจใคร หากแต่ต้องตรวจสอบอยู่เสมอ**

การพัฒนา Proposed Zero Trust Security Architecture แบบใหม่ที่เหมาะสมกับองค์กร เพื่อใช้เป็นแนวทางในรับมือกับความเสี่ยงและภัยคุกคามทางไซเบอร์นั้น ผู้วิจัยได้ศึกษาและอ้างอิงจาก Framework ต่าง ๆ อาทิ NIST Cybersecurity 2.0, Zero Trust, Security Mech และ COBIT 2019 นอกจากนี้ ยังศึกษา แนวปฏิบัติที่ดี (Best Practice Guidelines) เช่น CIS Critical Security Controls จาก SANS Institute รวมทั้งมาตรฐานอื่น ๆ ได้แก่ ISO 27001 และ ISO27002 เป็นต้น อย่างไรก็ตาม Proposed Zero Trust Security Architecture แบบใหม่ ที่ผู้วิจัยได้พัฒนาขึ้นมานี้ จะมีองค์ประกอบ 8 ส่วน รายละเอียด ดังในภาพประกอบที่ ง.1 ดังนี้



ภาพประกอบที่ ง.1 Proposed Zero Trust Security Architecture แบบใหม่

1. Endpoint (อุปกรณ์ปลายทาง) คือ การกำหนดให้อุปกรณ์ที่เข้าใช้งานต้องได้รับความยินยอมให้สามารถเข้าสู่ภายในระบบได้หรือมีความน่าเชื่อถือสามารถควบคุมให้เป็นมาตรฐานขององค์กรโดยได้ลงทะเบียนไว้กับองค์กรเรียบร้อยแล้ว

2. User & Password (ชื่อผู้ใช้และรหัสผ่าน) คือ การกำหนดรหัสผ่านตามหลัก Zero Trust นั้น มีหลายขั้นตอนและรวมถึงเงื่อนไขที่สำคัญที่ต้องปฏิบัติตาม เพื่อให้ระบบรักษาความมั่นคงปลอดภัยได้อย่างเต็มที่ ในการกำหนดรหัสผ่านตามหลัก Zero Trust ได้แก่

2.1 ความแข็งแกร่งของรหัสผ่าน คือ รหัสผ่านควรมีความยาวพอสมควรและมีความซับซ้อน เช่น การผสมตัวอักษรตัวพิมพ์ใหญ่และตัวเล็ก ตัวเลข และสัญลักษณ์พิเศษ เพื่อลดความเป็นไปได้ที่จะถูกทำลายโดยการโจมตีด้วยวิธีการคำนวณ

2.2 การเปลี่ยนรหัสผ่าน คือ ระบบควรบังคับให้ผู้ใช้เปลี่ยนรหัสผ่านอย่างสม่ำเสมอ เช่น ทุก 30 วันหรือตามนโยบายขององค์กร

2.3 การไม่ใช้รหัสผ่านที่ซ้ำมาแล้ว คือ ระบบควรไม่อนุญาตให้ใช้รหัสผ่านที่เคยใช้มาแล้ว เพื่อป้องกันการโจมตีด้วยวิธีการสุ่มลองครั้งหลังจากที่รหัสผ่านถูกเปิดเผย

2.4 การใช้ Multi-factor Authentication (MFA) คือ การใช้ MFA เพื่อเพิ่มชั้นความมั่นคงปลอดภัยโดยใช้วิธีการตรวจสอบตัวตนมากกว่าหนึ่งวิธี เช่น การใช้รหัสผ่านพร้อมกับรหัสยืนยันที่ถูกส่งไปยังโทรศัพท์เคลื่อนที่หรืออีเมล

3. Identity and Access Management (IAM) คือ กระบวนการหรือระบบที่ใช้ในการจัดการและควบคุมการเข้าถึงทรัพยากรต่าง ๆ ในระบบขององค์กร โดยมุ่งเน้นไปที่การรับรองตัวตนของผู้ใช้ และการควบคุมสิทธิ์การเข้าถึง เพื่อให้แน่ใจว่าเฉพาะผู้ที่มีสิทธิ์และเป็นผู้ยืนยันตัวตนได้เท่านั้นที่สามารถเข้าถึงข้อมูลและทรัพยากรได้ในองค์กร โดย IAM มักมีความสำคัญในระบบไอที และความมั่นคงปลอดภัยข้อมูล เป็นส่วนหนึ่งของการดำเนินงานที่มั่นคงปลอดภัยและมีประสิทธิภาพขององค์กรฟังก์ชันหลักของ Identity and Access Management ประกอบด้วย

3.1 Authentication (การรับรองตัวตน) คือ IAM ช่วยให้ระบบสามารถรับรองตัวตนของผู้ใช้ได้ โดยใช้หลายวิธี เช่น รหัสผ่าน การใช้งานบัตรประจำตัว หรือการใช้งานช่องสัญญาณไร้สาย (Biometrics) เพื่อให้แน่ใจว่าผู้ใช้คือผู้ที่ได้รับอนุญาตและยืนยันตัวตนได้

3.2 Authorization (การอนุญาต) คือ IAM ช่วยกำหนดสิทธิ์และการเข้าถึงทรัพยากรของระบบ โดยกำหนดสิทธิ์ของผู้ใช้ตามบทบาทหรือกลุ่มของผู้ใช้ ซึ่งช่วยให้แน่ใจว่าผู้ใช้งานมีการเข้าถึงเฉพาะข้อมูลและทรัพยากรที่เป็นไปตามนโยบายและความเหมาะสม

3.3 Administration (การบริหารจัดการ) คือ IAM ช่วยให้ผู้ใช้ดูแลระบบสามารถจัดการข้อมูลผู้ใช้ บทบาท และสิทธิ์การเข้าถึงได้อย่างมีประสิทธิภาพ รวมถึงการสร้าง การแก้ไข และการลบบัญชีผู้ใช้ การกำหนดสิทธิ์ และการจัดการข้อมูลอื่นๆ ที่เกี่ยวข้อง

3.4 Audit and Compliance (การตรวจสอบและความเป็นไปได้) IAM ช่วยให้สามารถตรวจสอบการเข้าถึงข้อมูลและทรัพยากร รวมถึงบันทึกกิจกรรมหรือเหตุการณ์การเข้าถึงเพื่อให้ปฏิบัติตามกฎระเบียบและมาตรฐานความมั่นคงปลอดภัย

3.5 Integration (การผสมผสาน) คือ IAM ช่วยให้ระบบสามารถผสมผสานกับแอปพลิเคชันและระบบอื่น ๆ ในองค์กรได้อย่างสมบูรณ์ เพื่อให้การจัดการตัวตนและการเข้าถึงทรัพยากรเป็นไปอย่างเรียบร้อยและมีประสิทธิภาพโดยรวมแล้ว Identity and Access Management (IAM) เป็นกลไกสำคัญที่ช่วยให้องค์กรสามารถจัดการและควบคุมการเข้าถึงทรัพยากรได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

4. Traffic (ข้อมูลการจราจร) การตรวจสอบและการตอบสนองทันทีต่อการจราจรและการเข้าถึงข้อมูลที่ไม่ถูกต้องหรือไม่เหมาะสมเป็นสิ่งสำคัญอย่างมากในสภาพแวดล้อมด้านความมั่นคงปลอดภัยของเครือข่ายอินเทอร์เน็ตและระบบสารสนเทศอื่น ๆ การเรียกใช้เทคโนโลยีการตรวจจับการบุกรุกและการจำกัดการเข้าถึงเป็นวิธีที่สำคัญในการตรวจสอบและป้องกันการบุกรุกจากบุคคลที่ไม่พึงประสงค์หรือการเข้าถึงทรัพยากรที่ไม่ได้รับอนุญาต ด้วยการใช้เทคโนโลยีนี้ ระบบสามารถตรวจจับการกระทำที่ไม่เหมาะสมหรือเกินกำหนดได้ทันที และมีการตอบสนองทันทีโดยการจำกัดหรือบล็อกการเข้าถึงทรัพยากรที่เสี่ยงต่อความมั่นคงปลอดภัย

นอกจากนี้ การตรวจสอบและการตอบสนองเหล่านี้มักจะเป็นเรื่องแม่นยำและอัตโนมัติในโหมดเรียลไทม์ เพื่อให้ระบบสามารถรับมือกับสถานการณ์ที่เปลี่ยนแปลงอย่างรวดเร็วและป้องกันอันตรายในเวลาที่เกิดขึ้นในทันทีทันใด การป้องกันอุบัติเหตุและการลดความเสี่ยงเป็นสิ่งสำคัญเพื่อให้ระบบทำงานอย่างมีประสิทธิภาพและมั่นคงในการให้บริการข้อมูลแก่ผู้ใช้งาน ในทางปฏิบัติ การใช้เทคโนโลยีการตรวจจับการบุกรุกและการจำกัดการเข้าถึงช่วยให้เครือข่ายและระบบสารสนเทศมั่นคงปลอดภัยและเสถียรภาพมากขึ้นในการดำเนินงานประจำวันขององค์กรและธุรกิจ

5. Control (การควบคุม) คือ การควบคุมแบบ Zero Trust เน้นการใช้นโยบายที่เข้มงวดและการควบคุมการเข้าถึงทรัพยากรอย่างเป็นระบบ โดยไม่ไว้วางใจตามหน้าที่หรือเครือข่ายที่ผู้ใช้งานจนถึงอุปกรณ์ที่ใช้เชื่อมต่อ โดยวิธีการควบคุมและปกป้องข้อมูลในรูปแบบ Zero Trust ดังนี้

5.1 Access Control (ควบคุมการเข้าถึง) เช่น กำหนดสิทธิ์การเข้าถึงโดยให้เข้าถึงทรัพยากรเฉพาะเฉพาะที่จำเป็นสำหรับการปฏิบัติงาน Principle of Least Privilege (POLP) การใช้ข้อมูลเกี่ยวกับตัวตนของผู้ใช้เพื่อกำหนดสิทธิ์การเข้าถึง Identity-Based Access Control (IBAC) ใช้เงื่อนไขต่างๆ Attribute-Based Access Control (ABAC) เช่น ตำแหน่ง หน้าที่ บทบาท และความสัมพันธ์ในการกำหนดสิทธิ์

5.2 Classification (การจัดหมวดหมู่ข้อมูล) เช่น การจัดหมวดหมู่ข้อมูลตามความลับและความเสี่ยง (Data Sensitivity Classification) เพื่อให้สามารถใช้นโยบายการเข้าถึงที่เข้มงวดและเชิงรุกภายในองค์กร กำหนดนโยบายในการจัดการข้อมูลตลอดจนถึงการทำลายข้อมูลในขั้นตอนการบริหารจัดการวงจรชีวิตของข้อมูล (Data Lifecycle Management)

5.3 Encryption (การเข้ารหัส) เช่น เข้ารหัสข้อมูลที่กำลังถูกส่งผ่านเครือข่าย (Data Encryption in Transit) เช่น การใช้ SSL/TLS สำหรับการเชื่อมต่อที่มั่นคงปลอดภัย เข้ารหัสข้อมูลที่อยู่ในการเก็บบันทึกหรือฐานข้อมูล (Data Encryption at Rest) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

อนึ่ง การควบคุมและป้องกันข้อมูลแบบ Zero Trust ช่วยให้องค์กรมีการควบคุมและความมั่นคงปลอดภัยที่เหมาะสมต่อการเข้าถึงข้อมูล โดยไม่วางใจตามแหล่งกำเนิดของข้อมูลหรือตำแหน่งที่มาของผู้ใช้หรืออุปกรณ์ นอกจากนี้ยังช่วยให้สามารถป้องกันการบุกรุกและการรั่วไหลข้อมูลได้อย่างมีประสิทธิภาพและมั่นคง

6. Assets (สินทรัพย์) คือ การจัดการทรัพยากรหรือ Assets แบบ Zero Trust เน้นการรับรองและควบคุมการเข้าถึงสินทรัพย์ทุกอย่างเคร่งครัด โดยไม่วางใจตามหน้าที่หรือเครือข่าย แนวคิดและวิธีการที่ใช้ในการจัดการสินทรัพย์ในรูปแบบ ดังนี้

6.1 การระบุและการจำแนกประเภทของสินทรัพย์ (Asset Identification and Classification) ระบุและจำแนกประเภทของสินทรัพย์ที่สำคัญตามลักษณะของแต่ละสินทรัพย์ เช่น ข้อมูลที่ละเอียด ระบบ เซิร์ฟเวอร์ และแอปพลิเคชัน

6.2 การตั้งค่านโยบายการเข้าถึง (Access Policy Setting) กำหนดนโยบายการเข้าถึงทรัพยากรอย่างเข้มงวดและโดยใช้หลักการ Zero Trust เพื่อให้มั่นใจว่าเฉพาะผู้ที่มีสิทธิ์เท่านั้นที่สามารถเข้าถึงได้

6.3 การใช้งานับตรระบบและการส่งข้อมูลโดยใช้การเข้ารหัส (Tokenization and Encryption) ใช้งานับตรผ่านบนระบบเพื่อรับรองตัวตนและใช้การเข้ารหัสข้อมูลเพื่อป้องกันการถูกแอบดักรับข้อมูลขณะการส่งผ่าน

6.4 การตรวจสอบและการวิเคราะห์ (Monitoring and Analysis) คือ การตรวจสอบและวิเคราะห์การเข้าถึงสินทรัพย์โดยตลอดเวลา เพื่อตรวจจับและตอบสนองต่อกิจกรรมที่ไม่ปกติ

6.5 การใช้งาน Identity and Access Management (IAM) คือ การใช้ระบบ IAM เพื่อจัดการตัวตนและการเข้าถึงของผู้ใช้ โดยใช้หลักการ Zero Trust เพื่อควบคุมการเข้าถึงสินทรัพย์

6.6 การสร้างและการบริหารจัดการนโยบาย (Policy Creation and Management) คือ การสร้างและการบริหารจัดการนโยบายการเข้าถึงทรัพยากรที่เข้มงวดและเชื่อถือได้ตามหลักการ Zero Trust

6.7 การป้องกันและการตอบสนองต่อการบุกรุก (Prevention and Response to Intrusions) คือ การใช้มาตรการป้องกันและการตอบสนองต่อการบุกรุกอย่างรวดเร็วและมีประสิทธิภาพเพื่อป้องกันและลดความเสี่ยงที่อาจเกิดขึ้น

การจัดการทรัพยากรแบบ Zero Trust ช่วยให้องค์กรมีความเชื่อมั่นในการควบคุมและความมั่นคงปลอดภัยของสินทรัพย์ที่สำคัญ โดยไม่วางใจตามหน้าที่หรือเครือข่าย และช่วยลดความเสี่ยงต่อการถูกบุกรุกหรือการรั่วไหลข้อมูลลงไปด้วย

7. SIEM คือการปรับใช้ SIEM (Security Information and Event Management) แบบ Zero Trust เน้นการตรวจสอบและวิเคราะห์ข้อมูลเกี่ยวกับความมั่นคงปลอดภัยและเหตุการณ์ที่เกิดขึ้นในระบบขององค์กร โดยใช้หลักการ Zero Trust เพื่อควบคุมและป้องกันการบุกรุกอย่างเฉพาะเจาะจงวิธีการปรับใช้ SIEM แบบ Zero Trust ดังนี้

7.1 การตรวจสอบและการวิเคราะห์โดยตลอดเวลา (Continuous Monitoring and Analysis) คือ ตรวจสอบและวิเคราะห์เหตุการณ์และกิจกรรมที่เกิดขึ้นในระบบขององค์กรอย่างต่อเนื่องโดยใช้หลักการ Zero Trust เพื่อตรวจจับและตอบสนองต่อการบุกรุกที่เกิดขึ้นได้อย่างรวดเร็ว

7.2 การตรวจสอบเหตุการณ์ข้ามเครือข่าย (Cross-Network Event Correlation) คือ การตรวจสอบและวิเคราะห์เหตุการณ์ที่เกิดขึ้นทั้งภายในและภายนอกเครือข่าย โดยใช้ข้อมูลจากแหล่งที่มาต่างๆ เพื่อค้นหาและตอบสนองต่อภัยคุกคามที่เกิดขึ้นในทุก ๆ มุมของระบบ

7.3 การใช้แนวทางการตอบสนองที่เชื่อถือได้ (Trusted Response Strategies) คือ การใช้แนวทางการตอบสนองต่อเหตุการณ์ที่ตรวจจับได้ โดยใช้วิธีการที่เชื่อถือได้และมีประสิทธิภาพเพื่อรักษาความมั่นคงปลอดภัยของระบบ

7.4 การตรวจสอบและการตอบสนองต่อการละเมิดการเข้าถึงแบบเรียลไทม์ (Real-time Detection and Response) คือ การตรวจสอบและการตอบสนองต่อการละเมิดอย่างรวดเร็วในขณะที่เกิดเหตุการรบกวนเกิดขึ้น เพื่อลดความเสี่ยงและความเสียหายที่อาจเกิดขึ้น

7.5 การสร้างและการบริหารจัดการนโยบาย (Policy Creation and Management) คือ การสร้างและการบริหารจัดการนโยบายการตรวจสอบและการตอบสนองต่อภัยคุกคามโดยใช้หลักการ Zero Trust เพื่อให้มั่นใจว่าระบบมีการควบคุมและความมั่นคงปลอดภัยที่เหมาะสม

8. Policy คือ การปรับใช้นโยบายแบบ Zero Trust เน้นการจัดการและควบคุมความเชื่อมั่นและความมั่นคงปลอดภัยของข้อมูลและทรัพยากรในระบบองค์กร โดยไม่วางใจตามตำแหน่งหรือบริบทที่เกิดขึ้น ด้วยวิธีการปรับใช้แต่ละนโยบาย ดังนี้

8.1 Governance (กำกับดูแลการดำเนินงาน) คือ สร้างกรอบการบริหารการดำเนินงานที่มีเครื่องมือและกระบวนการเพื่อควบคุมการเข้าถึงข้อมูลและทรัพยากร โดยใช้หลักการ Zero Trust เพื่อให้มั่นใจว่าการบริหารการดำเนินงานเป็นไปอย่างมีประสิทธิภาพและความมั่นคงปลอดภัย

8.2 Compliance (การปฏิบัติตามข้อบังคับ) คือ สร้างนโยบายการปฏิบัติตามข้อบังคับและมาตรฐานความมั่นคงปลอดภัยที่เกี่ยวข้อง โดยใช้หลักการ Zero Trust เพื่อให้การปฏิบัติตามข้อบังคับเป็นไปอย่างเข้มงวดและเชื่อถือได้

8.3 Security Assessment (การประเมินความมั่นคงปลอดภัย) คือ จัดทำการประเมินความมั่นคงปลอดภัยและการตรวจสอบเพื่อตรวจจับความเสี่ยงและช่องโหว่ในระบบ โดยใช้หลักการ Zero Trust เพื่อให้การประเมินความมั่นคงปลอดภัยเป็นไปอย่างอิสระและเชื่อถือได้

โปรดพิจารณาข้อความต่อไปนี้แล้วทำเครื่องหมาย ☒ ลงในช่องที่ตรงกับความจริง
ความคิดเห็น หรือความรู้สึกของท่านมากที่สุดเพียงช่องเดียวแบ่งระดับคำตอบเป็น 5 ระดับ ดังนี้

- | | | |
|---|---------|-------------------------------|
| 5 | หมายถึง | เหมาะสมหรือเห็นด้วยมากที่สุด |
| 4 | หมายถึง | เหมาะสมหรือเห็นด้วยมาก |
| 3 | หมายถึง | เหมาะสมหรือเห็นด้วยกลาง |
| 2 | หมายถึง | เหมาะสมหรือเห็นด้วยน้อย |
| 1 | หมายถึง | เหมาะสมหรือเห็นด้วยน้อยที่สุด |

ข้อที่	ข้อความ	ระดับความเหมาะสม				
		5	4	3	2	1
1	Proposed Zero Trust Security Architecture แบบใหม่ ที่พัฒนาขึ้น มีความเหมาะสมกับการนำไปใช้งานในองค์กร					
2	Proposed Zero Trust Security Architecture แบบใหม่ ที่พัฒนาขึ้น มีความครอบคลุมในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กร					
3	Proposed Zero Trust Security Architecture แบบใหม่ ที่พัฒนาขึ้น ไม่ซับซ้อนยุ่งยาก มีความเข้าใจง่ายต่อการนำไปใช้ในองค์กร					
4	Proposed Zero Trust Security Architecture แบบใหม่ ที่พัฒนาขึ้น จะสามารถปรับปรุงระดับความพร้อมทางไซเบอร์และรับมือกับความเล็งและภัยคุกคามทางไซเบอร์ในองค์กร					
5	Proposed Zero Trust Security Architecture แบบใหม่ ที่พัฒนาขึ้น สามารถพัฒนาระดับขีดความสามารถและมาตรฐานความมั่นคงปลอดภัยไซเบอร์ขององค์กร					

ส่วนที่ 3 ระดับความคิดเห็นโดยรวมของผู้ทรงคุณวุฒิที่มีต่อ Proposed Zero Trust Security Architecture แบบใหม่ ตามแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ใหม่ที่เหมาะสมกับองค์กร ภายใต้งานความคิดที่ไม่ไว้วางใจใคร หากแต่ต้องตรวจสอบเสมอ

3.1 “Proposed Zero Trust Security Architecture แบบใหม่ ที่พัฒนาขึ้น ตามแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมกับองค์กร ภายใต้งานความคิดที่ไม่ไว้วางใจใคร หากแต่ต้องตรวจสอบเสมอ” ตามภาพประกอบที่ ง.1 มีความเหมาะสมอยู่ในระดับใด

- () 5 เหมาะสมมากที่สุด
- () 4 เหมาะสมมาก
- () 3 เหมาะสมปานกลาง
- () 2 เหมาะสมน้อย
- () 1 เหมาะสมน้อยที่สุด

ข้อเสนอแนะอื่น ๆ เพื่อการปรับปรุง

.....

.....

3.2 “Proposed Zero Trust Security Architecture แบบใหม่ ที่พัฒนาขึ้น ตามแนวทางการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมกับองค์กร ภายใต้งานความคิดที่ไม่ไว้วางใจใคร หากแต่ต้องตรวจสอบเสมอ” ตามภาพประกอบที่ ง.1 มีการยอมรับอยู่ในระดับใด

- () 5 เหมาะสมมากที่สุด
- () 4 เหมาะสมมาก
- () 3 เหมาะสมปานกลาง
- () 2 เหมาะสมน้อย
- () 1 เหมาะสมน้อยที่สุด

ข้อเสนอแนะอื่น ๆ เพื่อการปรับปรุง

.....

.....

กราบขอบพระคุณที่ท่านได้กรุณาเสียสละเวลาอันมีค่าในการตอบแบบสอบถาม

ภาคผนวก จ

แบบประเมินความพึงพอใจของผู้ใช้แอปพลิเคชันสำหรับป้องกันและแจ้งเตือนภัย
คุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิค
การวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์



**แบบประเมินความพึงพอใจของผู้ใช้แอปพลิเคชันสำหรับป้องกันและแจ้งเตือนภัยคุกคาม
ทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์
ตอบสนองต่อภัยคุกคามแบบเรียลไทม์**

คำชี้แจง

แบบประเมินนี้ได้จัดทำขึ้นเพื่อสอบถามความพึงพอใจของผู้ใช้แอปพลิเคชันสำหรับป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ ซึ่งเป็นส่วนหนึ่งของการวิจัยในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

ผู้วิจัยจึงใคร่ขอความร่วมมือให้ท่านผู้ใช้แอปพลิเคชัน กรุณาตอบแบบสอบถามทุกข้อด้วยตัวของท่านเอง โดยให้ข้อมูล หรือแสดงความคิดเห็นที่ตรงกับความเป็นจริง ความรู้สึก หรือความคิดเห็นของท่านมากที่สุด ข้อมูลที่ได้จะนำไปใช้ประกอบการศึกษาและจะใช้เพื่อประโยชน์ทางวิชาการเท่านั้น ผู้วิจัยขอรับรองว่า จะไม่มีผลกระทบหรือก่อให้เกิดความเสียหายต่อตัวท่านแต่ประการใด ข้อคำถามในแบบสอบถาม แบ่งออกเป็น 3 ส่วน คือ

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบประเมิน

ส่วนที่ 2 ความพึงพอใจต่อการใช้งานแอปพลิเคชันสำหรับป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายที่มีความทนทานและความแม่นยำสูง

ส่วนที่ 3 ข้อเสนอแนะ

นาย กฤษ ศรีเงินดี, e-mail: kit.sringendee@gmail.com, โทรศัพท์: 081-626-1475
นักศึกษาหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
มหาวิทยาลัยศรีปทุม

การใช้งานเว็บแอปพลิเคชัน

ผู้วิจัย ได้พัฒนาระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์สำหรับการผ่านเว็บของระบบการตรวจหา วิเคราะห์ และตอบสนองต่อภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ (Security Information and Event Management: SIEM) ในรูปแบบเว็บแอปพลิเคชันที่สามารถทำงานได้ในอุปกรณ์ที่มีขนาดหน้าจอที่แตกต่างกัน สามารถทำงานได้บนทั้งแท็บเล็ตคอมพิวเตอร์ และคอมพิวเตอร์ทั่วไป ทั้งนี้ระบบสามารถรองรับจำนวนผู้ใช้ได้ไม่จำกัด โดยผู้ใช้สามารถเข้าใช้งานได้ที่ลิงก์ <https://xdr.siemkit.com> หรือ สแกนคิวอาร์โค้ด ดังภาพประกอบที่ จ.1



ภาพประกอบที่ จ.1 คิวอาร์โค้ดสำหรับเข้าใช้งานเว็บแอปพลิเคชันฯ

เมื่อผู้ใช้ ได้เข้าถึงแอปพลิเคชันนี้แล้ว จะพบในส่วนของการ Login เพื่อเข้าใช้งานตามที่ปรากฏใน ภาพประกอบที่ จ.2



ภาพประกอบที่ จ.2 ส่วนการ Login เพื่อเข้าใช้เว็บแอปพลิเคชันฯ

การประเมินแอปพลิเคชัน

ผู้วิจัยได้พัฒนาแบบประเมินออนไลน์ด้วย Google Form ซึ่งทุกท่าน สามารถเข้าตอบแบบสอบถาม ได้ที่ลิงก์ <https://forms.gle/RCQMxtN4iUuzUB528> หรือ สแกนคิวอาร์โค้ด ดังภาพประกอบที่ จ.3



ภาพประกอบที่ จ.3 คิวอาร์โค้ดสำหรับประเมินเว็บแอปพลิเคชันฯ

เมื่อทำการป้อนที่อยู่ของแบบประเมินออนไลน์ หรือสแกนคิวอาร์โค้ดเรียบร้อยแล้ว จะปรากฏดังภาพประกอบที่ จ.4

SPU
SRIPATUM
UNIVERSITY

คำชี้แจง

แบบประเมินนี้ ได้จัดทำขึ้นเพื่อสอบถามความพึงพอใจของผู้ใช้แอปพลิเคชันสำหรับป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย โดยใช้นักนิสิตภาควิชาสาระเทคโนโลยีคอมพิวเตอร์มาออกแบบเว็บไซต์ ซึ่งเป็นส่วนหนึ่งของงานวิจัยในทศวรรษที่ ๖ สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

ผู้วิจัยจึงใคร่ขอความร่วมมือให้ท่านผู้ใช้แอปพลิเคชัน กรุณาตอบแบบสอบถามทุกข้อด้วยความซื่อสัตย์ โดยให้ข้อมูล หรือแสดงความคิดเห็นที่ตรงกับความเป็นจริง ความรู้สึก หรือความคิดเห็นของท่านมากที่สุด ข้อมูลที่ได้จะนำไปใช้ประกอบการศึกษาและใช้เพื่อประโยชน์ทางวิชาการเท่านั้น ผู้วิจัยขอรับรองว่า จะไม่มีผลกระทบหรือก่อให้เกิดความเสียหายต่อตัวท่านแต่ประการใด ขอคำถามในแบบสอบถาม แบ่งออกเป็น ๖ ส่วน คือ

ส่วนที่ ๑ ข้อมูลทั่วไปของผู้ตอบแบบประเมิน

ส่วนที่ ๒ ความพึงพอใจต่อการใช้งานแอปพลิเคชันสำหรับป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายที่มีความเหมาะสมและความแม่นยำสูง

ส่วนที่ ๓ ข้อเสนอแนะ

ภาพประกอบที่ จ.4 หน้าแรกแบบประเมินแอปพลิเคชันฯ

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบประเมิน

1. เพศ

☐ ชาย

☐ หญิง

2. อายุ

☐ ต่ำกว่า 30 ปี

☐ 30-40 ปี

☐ 41-50 ปี

☐ 51 – 60 ปี

☐ 60 ปีขึ้นไป

3. ระดับการศึกษา

☐ ต่ำกว่าปริญญาตรี

☐ ปริญญาตรี

☐ ปริญญาโท

☐ ปริญญาเอก

4. ระยะเวลาของประสบการณ์ที่ท่านได้ทำงานในสายงานของท่าน

☐ น้อยกว่า 3 ปี

☐ 3-5 ปี

☐ 6-10 ปี

☐ มากกว่า 10 ปี

5. ประเภทหน่วยงานของท่าน

☐ ภาครัฐ

☐ ภาคเอกชน

☐ ภาครัฐวิสาหกิจ

☐ อื่นๆ

6. หน่วยงานของท่านดำเนินงานด้านใด

☐ บริการ

☐ ผลิตภัณฑ์

☐ การค้า

☐ อื่นๆ

ส่วนที่ 2 ระดับความพึงพอใจต่อการใช้งานแอปพลิเคชันสำหรับป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนคอมพิวเตอร์แม่ข่ายฯ

ขอความกรุณาท่านได้โปรดพิจารณาข้อคำถามดังต่อไปนี้ แล้วทำเครื่องหมาย ☒ ลงในช่องที่ตรงกับความจริง ความคิดเห็น หรือความรู้สึกรของท่านมากที่สุดเพียงช่องเดียว ทั้งนี้ผู้วิจัยได้แบ่งระดับคำตอบไว้เป็น 5 ระดับ ดังนี้

5 หมายถึง ระดับพึงพอใจมากที่สุด

4 หมายถึง ระดับพึงพอใจมาก

3 หมายถึง ระดับพึงพอใจปานกลาง

2 หมายถึง ระดับพึงพอใจน้อย

1 หมายถึง ระดับพึงพอใจน้อยที่สุด

ข้อที่	ข้อความคำถาม	ระดับความพึงพอใจ				
		5	4	3	2	1
ด้านระบบตรงกับความต้องการของผู้ใช้						
1	ความสามารถของระบบในการจัดการแจ้งเตือนการโจมตีทางไซเบอร์ได้อย่างรวดเร็ว					
2	ความสามารถของระบบในการจัดการป้องกันการโจมตีทางไซเบอร์ได้อย่างรวดเร็ว					
3	ความสามารถของระบบในการแสดงข้อมูลได้อย่างรวดเร็ว					
4	ความสามารถของระบบในการค้นหาข้อมูลได้อย่างถูกต้อง					
5	ความถูกต้องและแม่นยำในการป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์ที่ทำงานแบบเรียลไทม์					
ด้านการทำงานได้ตามฟังก์ชันงานของระบบ						
1	ความสามารถในการเชื่อมโยงข้อมูลกับระบบอินเทอร์เน็ตประสานสรรพสิ่ง					
2	ความสามารถในการจัดการข้อมูล Log System ได้ถูกต้อง					
3	ความสามารถในการจัดการแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย					
4	ความสามารถในการจัดการป้องกันเครื่องคอมพิวเตอร์แม่ข่าย					
5	ความสามารถในการจัดการประมวลผลได้อย่างเรียลไทม์					
ด้านความง่ายต่อการใช้งานระบบ						
1	รูปแบบการใช้งานระบบ มีความเข้าใจง่ายในการเข้าถึงข้อมูล					
2	ขั้นตอนการใช้งานง่าย เมนูไม่ซับซ้อน					
3	ความเหมาะสมในการวางตำแหน่งของส่วนประกอบบนจอภาพ					
4	ระบบมีความเหมาะสมที่จะใช้ในหน่วยงานของท่าน					
5	ระบบมีความเหมาะสมที่จะนำไปปรับใช้กับ SME					

ข้อที่	ข้อความถาม	ระดับความพึงพอใจ				
		5	4	3	2	1
ด้านประสิทธิภาพการทำงานของระบบ						
1	ความสามารถในการใช้งานและบันทึกข้อมูลของ Log System					
2	ความสามารถของระบบในส่วนของการบันทึกข้อมูล					
3	ความสามารถของระบบในส่วนของการแก้ไขเงื่อนไขการป้องกันภัยคุกคามทางไซเบอร์					
4	ความสามารถของระบบในส่วนของการป้องกันการลบข้อมูล					
5	ความสามารถของระบบในส่วนของการแสดงผลข้อมูล					
ด้านความปลอดภัยของระบบ						
1	ความเหมาะสมในการกำหนดสิทธิ์ของผู้ใช้ได้ตามที่					
2	มีระบบ Login / Logout เพื่อตรวจสอบผู้เข้าใช้ระบบ					
3	มีระบบการเข้ารหัสและถอดรหัสเพื่อส่งผ่านข้อมูลระหว่างหน้าจอ					
4	มีกลไกการเปลี่ยนรหัสผู้ใช้งานให้มีความมั่นคงปลอดภัยไซเบอร์ภายในระบบ					
5	ความเหมาะสมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบ					

ส่วนที่ 3 ข้อเสนอแนะอื่น ๆ และสิ่งที่ควรปรับปรุงแก้ไขเพิ่มเติม

.....

.....

.....

.....

.....

.....

.....

ภาคผนวก จ

ข้อมูลประวัติผู้ทรงคุณวุฒิ

ข้อมูลประวัติผู้ทรงคุณวุฒิทางด้านเทคโนโลยีดิจิทัล

ลำดับที่	ชื่อ-สกุล	ประวัติผู้ทรงคุณวุฒิ
1	ผศ.ดร.สุนิษา คัดใจเดียว	ผศ.ดร.สุนิษา คัดใจเดียว ตำแหน่ง : ประธานหลักสูตร สาขาวิชาเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล หน่วยงาน : มหาวิทยาลัยราชภัฏนครศรีธรรมราช ประวัติการศึกษา : ปริญญาเอก ปรัชญาคุษฎีบัณฑิต (เทคโนโลยีสารสนเทศ) มหาวิทยาลัยศรีปทุม 2562 ปริญญาโท วิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ มหาวิทยาลัยวลัยลักษณ์ 2553 ปริญญาตรีวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยราชภัฏนครศรีธรรมราช
2	ผศ.ดร.ลำราญ ไชยคำวัง	ตำแหน่ง : ผู้ช่วยศาสตราจารย์ หน่วยงาน : มหาวิทยาลัยราชภัฏเชียงราย ประวัติการศึกษา : ปริญญาเอก ปรัชญาคุษฎีบัณฑิต (เทคโนโลยีสารสนเทศ) มหาวิทยาลัยศรีปทุม 2566 ปริญญาโท วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏเชียงราย 2554 ปริญญาตรี วิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยราชภัฏเชียงราย 2538

ลำดับที่	ชื่อ-สกุล	ประวัติผู้ทรงคุณวุฒิ
3	ผศ.ดร.ชัยพร ทบแป	ตำแหน่ง : ผู้จัดการศูนย์นวัตกรรมดิจิทัล หน่วยงาน : บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ประวัติการศึกษา : ปริญญาเอก ปรัชญาดุษฎีบัณฑิต (เทคโนโลยีสารสนเทศ) มหาวิทยาลัยศรีปทุม 2562 ปริญญาโท วิศวกรรมศาสตรมหาบัณฑิต (โลจิสติกส์และโซ่อุปทาน) มหาวิทยาลัยมหิดล 2562 ปริญญาโท บริหารธุรกิจมหาบัณฑิต มหาวิทยาลัยรามคำแหง 2547 ปริญญาตรี รัฐประศาสนศาสตรบัณฑิต มหาวิทยาลัยสุโขทัยธรรมมาธิราช 2542 ปริญญาตรี วิทยาศาสตร์บัณฑิต (คอมพิวเตอร์) มหาวิทยาลัยรามคำแหง 2535
4	ดร. เอกนัฏ ป้ายคล้อย	ตำแหน่ง : ประธานกรรมการ หน่วยงาน : บริษัท EP&IT Solution Co., Ltd. ประวัติการศึกษา : ปริญญาเอก ปรัชญาดุษฎีบัณฑิต (เทคโนโลยีสารสนเทศ) มหาวิทยาลัยศรีปทุม 2562 ปริญญาโท วิทยาศาสตร์มหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม 2545 ปริญญาตรี วิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมไฟฟ้า (ไฟฟ้ากำลัง) มหาวิทยาลัยศรีปทุม 2542

ลำดับที่	ชื่อ-สกุล	ประวัติผู้ทรงคุณวุฒิ
5	ดร. เกรียงไกร ภูวนิชย์	ตำแหน่ง : รองประธานคณะกรรมการสาขาวิศวกรรมคอมพิวเตอร์ หน่วยงาน : วิศวกรรมสถานแห่งประเทศไทยในพระบรมราชูปถัมภ์ (วสท) ประวัติการศึกษา : ปริญญาเอก ปรัชญาคุษฎีบัณฑิต (เทคโนโลยีสารสนเทศ) มหาวิทยาลัยศรีปทุม 2567 ปริญญาโท บริหารธุรกิจมหาบัณฑิต สถาบันบัณฑิตบริหารธุรกิจศศินทร์แห่งจุฬาลงกรณ์มหาวิทยาลัย 2540 ปริญญาโท บริหารธุรกิจมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย 2538 ปริญญาโท วิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์ University of Southern California, Los Angeles, California, USA. 2536 ปริญญาตรี วิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมอิเล็กทรอนิกส์ (เกียรตินิยมอันดับ 1) Northrop University, Los Angeles, California, USA. 2527 ปริญญาตรี วิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมไฟฟ้า มหาวิทยาลัยเกษตรศาสตร์ 2525

ลำดับที่	ชื่อ-สกุล	ประวัติผู้ทรงคุณวุฒิ
6	ดร. เทพฤทธิ์ พระเทพ	ตำแหน่ง : วิศวกรเทคโนโลยี ฝ่ายวิเคราะห์และออกแบบ หน่วยงาน : บริษัท NEYAA Inc. Group ประวัติการศึกษา : ปริญญาเอก ปรัชญาดุษฎีบัณฑิต (เทคโนโลยีสารสนเทศ) มหาวิทยาลัยศรีปทุม 2566 ปริญญาโท วิศวกรรมศาสตรมหาบัณฑิต วิศวกรรมโครงสร้าง และวิศวกรรมปฐพี มหาวิทยาลัยรังสิต 2557 ปริญญาโท นิเทศศาสตรมหาบัณฑิต สาขาประชาสัมพันธ์ มหาวิทยาลัยศรีปทุม 2544 ปริญญาตรี อดุสากรรมศาสตรบัณฑิต สาขาวิศวกรรมโยธา มหาวิทยาลัยศรีปทุม 2540

ภาคผนวก ข

หนังสือที่ออกจากมหาวิทยาลัย

**BANGKOK**

2410/2
PHAHOLYOTHIN RD.,
JATUJAK, BANGKOK
10900
TEL. 0 2579 1111
FAX. 0 2561 1721
www.spu.ac.th

CHONBURI CAMPUS

79 BANGNA-TRAD RD.,
KLONGTAMRU, MUANG
CHONBURI 20000
TEL. 0 3874 3690-9
FAX. 0 3874 3700
www.eest.spu.ac.th

KHON KAEN

182/13 MOO 4,
SRICHAN RD.,
NAIMUANG DISTRICT,
AMPHUR MUANG,
KHON KAEN 40000
TEL. 0 4322 4111
FAX. 0 4322 4119
www.khonkaen.spu.ac.th

ที่ มคอ.0110/49๓

30 พฤษภาคม 2567

เรื่อง ขอความอนุเคราะห์ประเมินความเหมาะสมของ Proposed Zero Trust Security Architecture

เรียน ผู้ช่วยศาสตราจารย์ ดร.สุณิษา คัดใจเดียว

สิ่งที่แนบมา : แบบประเมิน

ด้วย นายกฤษ ศรีเงินดี นักศึกษาระดับปริญญาโท รหัสนักศึกษา 66501988 หลักสูตร
วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
อยู่ระหว่างการทำวิทยานิพนธ์ เรื่อง "การพัฒนาแบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่อง
คอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์" โดยมี ผู้ช่วย
ศาสตราจารย์ ดร.สุรศักดิ์ มั่งสิงห์ เป็นอาจารย์ที่ปรึกษา และศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง เป็น
อาจารย์ที่ปรึกษาร่วม



เพื่อให้การดำเนินการทำวิจัยเป็นไปตามวัตถุประสงค์ของการศึกษา ทางหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม จึงเรียนมาเพื่อขอความ
อนุเคราะห์จากท่าน ประเมินความเหมาะสมของ Proposed Zero Trust Security Architecture ตามสิ่งที่แนบ
มาด้วยนี้ อย่างไรก็ตาม หากท่านมีความประสงค์ จะทราบรายละเอียดเพิ่มเติม กรุณาประสานงานกับผู้วิจัยได้
โดยตรง ทางหมายเลขโทรศัพท์ 081-626-1475 ไลน์ไอดีเล็กทรอนิกส์ : kit.sringendee@gmail.com

จึงเรียนมาเพื่อโปรดทราบและพิจารณาให้ความอนุเคราะห์ตอบแบบประเมินมา ณ โอกาสนี้ด้วย จัก
ขอบคุณยิ่ง

ขอแสดงความนับถือ



(ผู้ช่วยศาสตราจารย์ ดร.ปราณี มณีวิรัตน์)
คณบดีคณะเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ
โทร. 02 579 1111 ต่อ 2196



BANGKHEN
2410/2
PHAHOLYOTHIN RD.
JATUJAK, BANGKOK
10900
TEL. 0 2579 1111
FAX. 0 2561 1721
www.spu.ac.th

CHONBURI CAMPUS
79 BANGNA-TRAD RD.
KLONGTAMRU, MUANG
CHONBURI 20000
TEL. 0 3874 3690-9
FAX. 0 3874 3700
www.east.spu.ac.th

KHON KAEN
182/12 MOO 4,
SRICHAN RD.,
NAIMUANG DISTRICT,
AMPHUR MUANG,
KHON KAEN 40000
TEL. 0 4322 4111
FAX. 0 4322 4119
www.khonkaen.spu.ac.th

ที่ มสป.0110/459

30 พฤษภาคม 2567

เรื่อง ขอความอนุเคราะห์ประเมินความเหมาะสมของ Proposed Zero Trust Security Architecture

เรียน ผู้ช่วยศาสตราจารย์ ดร.สำราญ ไชยคำวงศ์

สิ่งที่แนบมา : แบบประเมิน

ด้วย นายกฤษ ศรีเจินดี นักศึกษาระดับปริญญาโท รหัสนักศึกษา 66501988 หลักสูตร
วิทยาศาสตร์มหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
อยู่ระหว่างการทำวิทยานิพนธ์ เรื่อง "การพัฒนาระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่อง
คอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์" โดยมี ผู้ช่วย
ศาสตราจารย์ ดร.สุรศักดิ์ มั่งสิงห์ เป็นอาจารย์ที่ปรึกษา และศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง เป็น
อาจารย์ที่ปรึกษาร่วม



เพื่อให้การดำเนินการทำวิจัยเป็นไปตามวัตถุประสงค์ของการศึกษา ทางหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม จึงเรียนมาเพื่อขอความ
อนุเคราะห์จากท่าน ประเมินความเหมาะสมของ Proposed Zero Trust Security Architecture ตามสิ่งที่แนบ
มาด้วยนี้ อย่างไรก็ตาม หากท่านมีความประสงค์ จะทราบรายละเอียดเพิ่มเติม กรุณาประสานงานกับผู้วิจัยได้
โดยตรง ทางหมายเลขโทรศัพท์ 081-626-1475 ไปรษณีย์อิเล็กทรอนิกส์ : kit.sringendee@gmail.com

จึงเรียนมาเพื่อโปรดทราบและพิจารณาให้ความอนุเคราะห์ตอบแบบประเมินมา ณ โอกาสนี้ด้วย จัก
ขอบคุณยิ่ง

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.ปราณี มณีรัตน์)
คณบดีคณะเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ
โทร. 02 579 1111 ต่อ 2196

**BANGKOK**

2410/2
PHAHOLYOTHIN RD.,
JATUJAK, BANGKOK
10900
TEL. 0 2579 1111
FAX. 0 2561 1721
www.spu.ac.th

CHONBURI CAMPUS

79 BANGNA-TRAD RD.,
KLONGTAMRU, MUANG,
CHONBURI 20000
TEL. 0 3874 3690-9
FAX. 0 3874 3700
www.east.spu.ac.th

KHON KAEN

182/12 MOO 4,
SRICHAN RD.,
NAI MUANG DISTRICT,
AMPHUR MUANG,
KHON KAEN 40000
TEL. 0 4322 4111
FAX. 0 4322 4119
www.khonkaen.spu.ac.th

ที่ มศป.0110/439

30 พฤษภาคม 2567

เรื่อง ขอความอนุเคราะห์ประเมินความเหมาะสมของ Proposed Zero Trust Security Architecture

เรียน ผู้ช่วยศาสตราจารย์ ดร.ชัยพร ทบแป

สิ่งที่แนบมา : แบบประเมิน

ด้วย นายกฤษ ศรีเงินดี นักศึกษาระดับปริญญาโท รหัสนักศึกษา 66501988 หลักสูตร
วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
อยู่ระหว่างการทำวิทยานิพนธ์ เรื่อง "การพัฒนากรอบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่อง
คอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์" โดยมี ผู้ช่วย
ศาสตราจารย์ ดร.สุรศักดิ์ มั่งสิงห์ เป็นอาจารย์ที่ปรึกษา และศาสตราจารย์ ดร.ประสงค์ ปราณิตพลกรัง เป็น
อาจารย์ที่ปรึกษาร่วม



เพื่อให้การดำเนินการทำวิจัยเป็นไปตามวัตถุประสงค์ของการศึกษา ทางหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม จึงเรียนมาเพื่อขอความ
อนุเคราะห์จากท่าน ประเมินความเหมาะสมของ Proposed Zero Trust Security Architecture ตามสิ่งที่แนบ
มาด้วยนี้ อย่างไรก็ตาม หากท่านมีความประสงค์ จะทราบรายละเอียดเพิ่มเติม กรุณาประสานงานกับผู้วิจัยได้
โดยตรง ทางหมายเลขโทรศัพท์ 081-626-1475 ไปรษณีย์อิเล็กทรอนิกส์ : kitsringendee@gmail.com

จึงเรียนมาเพื่อโปรดทราบและพิจารณาให้ความอนุเคราะห์ตอบแบบประเมินมา ณ โอกาสนี้ด้วย จัก
ขอบคุณยิ่ง

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.ปราณี มณีรัตน์)
คณบดีคณะเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ
โทร. 02 579 1111 ต่อ 2196

BANGKHEN
2410/2
PHAKOLYOTHIN RD.,
JATUJAK, BANGKOK
10900
TEL. 0 2579 1111
FAX. 0 2561 1721
www.spu.ac.th

CHONBURI CAMPUS
79 BANGNA-TRAD RD.,
KLONGTAMRU, MUANG
CHONBURI 20000
TEL. 0 3874 3690-9
FAX. 0 3874 3700
www.east.spu.ac.th

KHON KAEN
182/12 MOO 4,
SRICHAN RD.,
NAIMUANG DISTRICT,
AMPHUR MUANG,
KHON KAEN 40000
TEL. 0 4322 4111
FAX. 0 4322 4119
www.khonkaen.spu.ac.th

ที่ มสป.0110/459

30 พฤษภาคม 2567

เรื่อง ขอความอนุเคราะห์ประเมินความเหมาะสมของ Proposed Zero Trust Security Architecture

เรียน ดร.เอกฉัตร ปายคล้อย

สิ่งที่แนบมา : แบบประเมิน

ด้วย นายกฤษ ศรีเงินดี นักศึกษาระดับปริญญาโท รหัสนักศึกษา 66501988 หลักสูตร
วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
อยู่ระหว่างการทำวิทยานิพนธ์ เรื่อง "การพัฒนาระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่อง
คอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์" โดยมี ผู้ช่วย
ศาสตราจารย์ ดร.สุรศักดิ์ มั่งสิงห์ เป็นอาจารย์ที่ปรึกษา และศาสตราจารย์ ดร.ประสงค์ ปรานีพิตรกรัง เป็น
อาจารย์ที่ปรึกษาร่วม



เพื่อให้การดำเนินการทำวิจัยเป็นไปตามวัตถุประสงค์ของการศึกษา ทางหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม จึงเรียนมาเพื่อขอความ
อนุเคราะห์จากท่าน ประเมินความเหมาะสมของ Proposed Zero Trust Security Architecture ตามสิ่งที่แนบ
มาด้วยนี้ อย่างไรก็ตาม หากท่านมีความประสงค์ จะทราบรายละเอียดเพิ่มเติม กรุณาประสานงานกับผู้วิจัยได้
โดยตรง ทางหมายเลขโทรศัพท์ 081-626-1475 ไปรษณีย์อิเล็กทรอนิกส์ : kitsringendee@gmail.com

จึงเรียนมาเพื่อโปรดทราบและพิจารณาให้ความอนุเคราะห์ตอบแบบประเมินมา ณ โอกาสนี้ด้วย จัก
ขอบคุณยิ่ง

ขอแสดงความนับถือ

(Signature)

(ผู้ช่วยศาสตราจารย์ ดร.ปราณี มณีรัตน์)
คณบดีคณะเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ
โทร. 02 579 1111 ต่อ 2196

**BANGKOK**

2410/2
PHAHOLYOTHIN RD.,
JATUJAK, BANGKOK
10900
TEL. 0 2579 1111
FAX. 0 2561 1721
www.spu.ac.th

CHONBURI CAMPUS

79 BANGNA-TRAD RD.,
KLONGTAMRU, MUANG,
CHONBURI 30000
TEL. 0 3874 5690-8
FAX. 0 3874 5700
www.east.spu.ac.th

KHON KAEN

182/12 MOO 4,
SRICHAN RD.,
NAIMUANG DISTRICT,
AMPHUR MUANG,
KHON KAEN 40000
TEL. 0 4322 4111
FAX. 0 4322 4119
www.khonkaen.spu.ac.th

ที่ มคอ.0110/489

30 พฤษภาคม 2567

เรื่อง ขอความอนุเคราะห์ประเมินความเหมาะสมของ Proposed Zero Trust Security Architecture
เรียน ดร.เทพฤทธิ์ พระเทพ
สิ่งที่แนบมา : แบบประเมิน

ด้วย นายคุณ ศรีเงินดี นักศึกษาระดับปริญญาโท รหัสนักศึกษา 66501988 หลักสูตร
วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
อยู่ระหว่างการทำวิทยานิพนธ์ เรื่อง “การพัฒนาระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่อง
คอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์” โดยมี ผู้ช่วย
ศาสตราจารย์ ดร.สุรศักดิ์ มั่งลิ้งห์ เป็นอาจารย์ที่ปรึกษา และศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง เป็น
อาจารย์ที่ปรึกษาร่วม



เพื่อให้การดำเนินการทำวิจัยเป็นไปตามวัตถุประสงค์ของการศึกษา ทางหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม จึงเรียนมาเพื่อขอความ
อนุเคราะห์จากท่าน ประเมินความเหมาะสมของ Proposed Zero Trust Security Architecture ตามสิ่งที่แนบ
มาด้วยนี้ อย่างไรก็ตาม หากท่านมีความประสงค์ จะทราบรายละเอียดเพิ่มเติม กรุณาประสานงานกับผู้วิจัยได้
โดยตรง ทางหมายเลขโทรศัพท์ 081-626-1475 ไลน์ไอดีเล็กทรอนิกส์ : kit.sringendee@gmail.com

จึงเรียนมาเพื่อโปรดทราบและพิจารณาให้ความอนุเคราะห์ตอบแบบประเมินมา ณ โอกาสนี้ด้วย จัก
ขอบคุณยิ่ง

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.ปราณี มณีรัตน์)
คณบดีคณะเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ
โทร. 02 579 1111 ต่อ 2196

**BANGKOK**

2410/2
PHAHOLYOTHIN RD.,
JATUJAK, BANGKOK
10900
TEL. 0 2579 1111
FAX. 0 2561 1721
www.spu.ac.th

CHONBURI CAMPUS

79 BANGNA-TRAD RD.,
KLONGTAMRU, MUANG,
CHONBURI 20000
TEL. 0 3874 3690-9
FAX. 0 3874 3700
www.east.spu.ac.th

KHON KAEN

182/12 KMO 4,
SRICHAN RD.,
NAIMUANG DISTRICT,
AMPHUR MUANG,
KHON KAEN 40000
TEL. 0 4322 4111
FAX. 0 4322 4119
www.khonkaen.spu.ac.th

ที่ มคอ.0110/434

30 พฤษภาคม 2567

เรื่อง ขออนุญาตเสนอประเมินความเหมาะสมของ Proposed Zero Trust Security Architecture

เรียน ดร.เกรียงไกร อุวณิชชัย

สิ่งที่แนบมา: แบบประเมิน

ด้วย นายกุลฐ ศรีเงินดี นักศึกษาระดับปริญญาโท รหัสนักศึกษา 66501988 หลักสูตร
วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
อยู่ระหว่างการทำวิทยานิพนธ์ เรื่อง "การพัฒนาระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่อง
คอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์" โดยมี ผู้ช่วย
ศาสตราจารย์ ดร.สุรศักดิ์ มั่งสิงห์ เป็นอาจารย์ที่ปรึกษา และศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง เป็น
อาจารย์ที่ปรึกษาร่วม



เพื่อให้การดำเนินการทำวิทยานิพนธ์เป็นไปตามวัตถุประสงค์ของการศึกษา ทางหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม จึงเรียนมาเพื่อขอความ
อนุเคราะห์จากท่าน ประเมินความเหมาะสมของ Proposed Zero Trust Security Architecture ตามสิ่งที่แนบ
มาด้วยนี้ อย่างไรก็ตาม หากท่านมีความประสงค์ จะทราบรายละเอียดเพิ่มเติม กรุณาประสานงานกับผู้วิจัยได้
โดยตรง ทางหมายเลขโทรศัพท์ 081-626-1475 ไปรษณีย์อิเล็กทรอนิกส์ : kits.sringendee@gmail.com

จึงเรียนมาเพื่อโปรดทราบและพิจารณาให้ความอนุเคราะห์ตอบแบบประเมินมา ณ โอกาสนี้ด้วย จัก
ขอบคุณยิ่ง

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.ปราณี มณีรัตน์)
คณบดีคณะเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ
โทร. 02 579 1111 ต่อ 2196

ภาคผนวก ข

หนังสือรับรองการใช้ประโยชน์



หนังสือรับรองการใช้ประโยชน์ผลงานวิจัย

มหาวิทยาลัยศรีปทุม

ข้าพเจ้า (นาย/นาง/นางสาว) ศิริระ นกยูงทอง
 ตำแหน่ง หัวหน้างาน ชื่อหน่วยงาน สำนักงานส่งเสริมเศรษฐกิจดิจิทัล
 สถานที่ตั้ง 80 ซ.ลาดพร้าว4 แขวงจอมพล เขตจตุจักร กทม
 โทรศัพท์ 0861060361 Email sira.no@depa.or.th

ขอรับรองว่าได้นำผลงานทางวิชาการ/วิจัยเรื่อง/งานสร้างสรรค์ เรื่อง การพัฒนาระบบป้องกัน
 และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์
 ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ โดยมีซึ่งเป็นของ นาย กลุณ ศรีเงินดี มาใช้ประโยชน์ในองค์กร/
 หน่วยงาน/กลุ่มของข้าพเจ้า โดยใช้ในระหว่างวันที่ 23 พ.ค. 2567 ถึงวันที่ 23 พ.ค. 2567
 ก่อให้เกิดผลดีในด้านต่อไปนี้ (ท่านเครื่องหมาย ☒ เลือกได้มากกว่า 1 ข้อ)

- ☐ การใช้ประโยชน์เชิงวิชาการ ☒ การใช้ประโยชน์เชิงสาธารณะ
☐ การใช้ประโยชน์เชิงนโยบาย ☒ การใช้ประโยชน์เชิงพาณิชย์
☐ การใช้ประโยชน์ทางอื่น

(โปรดระบุรายละเอียด)

ข้าพเจ้าขอลงนาม ในหนังสือรับรองการนำไปใช้ประโยชน์ด้วยความจริงทุกประการ เพื่อเป็นหลักฐาน
 การประโยชน์จากผลงานวิจัยหรืองานสร้างสรรค์ ของ นาย กลุณ ศรีเงินดี

ลงลายมือชื่อ

(ศิริระ นกยูงทอง)

วันที่ 23 / พ.ค. / 2567



หนังสือรับรองการใช้ประโยชน์ผลงานวิจัย

มหาวิทยาลัยศรีปทุม

ข้าพเจ้า (นาย/นาง/นางสาว) คณพอล ทงสว่างราษฎร์
 ตำแหน่ง ผู้อำนวยการศูนย์วิจัยและพัฒนาการเกษตร
 สถานที่ตั้ง สำนักงานเกษตรอำเภอเมือง
 โทรศัพท์ 2718000 (8042) Email khanaphot.h@oag.go.th

ขอรับรองว่าได้นำผลงานทางวิชาการ/วิจัยเรื่อง/งานสร้างสรรค์ เรื่อง การพัฒนาระบบป้องกัน
 และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย โดยใช้เทคนิคการวิเคราะห์เหตุการณ์
 ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ โดยมีชื่อเป็นของ นาย กฤษ ศรีเงินดี มาใช้ประโยชน์ในองค์กร/
 หน่วยงาน/กลุ่มของข้าพเจ้า โดยไว้ในระหว่างวันที่ 23/05/2566 ถึงวันที่ 24/05/2566

ก่อให้เกิดผลดีในด้านต่อไปนี้ (ทำเครื่องหมาย ☒ เลือกได้มากกว่า 1 ข้อ)

- ☒ การใช้ประโยชน์เชิงวิชาการ ☒ การใช้ประโยชน์เชิงสาธารณะ
☒ การใช้ประโยชน์เชิงนโยบาย ☐ การใช้ประโยชน์เชิงพาณิชย์
☐ การใช้ประโยชน์ทางอื่น

(โปรดระบุรายละเอียด).....

ข้าพเจ้าขอลงนาม ในหนังสือรับรองการนำไปใช้ประโยชน์ด้วยความจริงทุกประการ เพื่อเป็นหลักฐาน
 การประโยชน์จากผลงานวิจัยหรืองานสร้างสรรค์ ของ นาย กฤษ ศรีเงินดี

ลงลายมือชื่อ คณ พ.

(นายคณพอล ทงสว่างราษฎร์
 วันที่ 14/5/2566)



หนังสือรับรองการใช้ประโยชน์ผลงานวิจัย
มหาวิทยาลัยศรีปทุม

ข้าพเจ้า (นาย/นาง/นางสาว)..... ปิยวัฒน์ แพร่งสุวรรณไ
ตำแหน่ง IT Manager ชื่อหน่วยงาน ITD
สถานที่ตั้ง 238/7 ถนนอโศก-ดินแดง แขวงบางกะปิ เขตห้วยขวาง กรุงเทพฯ 10310
โทรศัพท์ 06414611 Email piyawat.p@bemplc.co.th

ขอรับรองว่าได้นำผลงานทางวิชาการ/วิจัยเรื่อง/งานสร้างสรรค์ เรื่อง การพัฒนาระบบป้องกัน
และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย โดยใช้เทคนิคการวิเคราะห์เหตุการณ์
ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ โดยมีซึ่งเป็นของ นาย กฤษ ศรีจินดี มาใช้ประโยชน์ในองค์กร/
หน่วยงาน/กลุ่มของข้าพเจ้า โดยใช้ในระหว่างวันที่ 24/5/67 ถึงวันที่ 31/5/67

ก่อให้เกิดผลดีในด้านต่อไปนี้ (ทำเครื่องหมาย ☒ เลือกได้มากกว่า 1 ข้อ)

- ☒ การใช้ประโยชน์เชิงวิชาการ ☒ การใช้ประโยชน์เชิงสาธารณะ
☐ การใช้ประโยชน์เชิงนโยบาย ☒ การใช้ประโยชน์เชิงพาณิชย์
☐ การใช้ประโยชน์ทางอื่น

(โปรดระบุรายละเอียด).....

ข้าพเจ้าขอลงนาม ในหนังสือรับรองการนำไปใช้ประโยชน์ด้วยความจริงทุกประการ เพื่อเป็นหลักฐาน
การประโยชน์จากผลงานวิจัยหรืองานสร้างสรรค์ ของ นาย กฤษ ศรีจินดี

ลงลายมือชื่อ..... ปิยวัฒน์
(ปิยวัฒน์ แพร่งสุวรรณไ)
วันที่ 31 , 5 , 67



หนังสือรับรองการใช้ประโยชน์ผลงานวิจัย

มหาวิทยาลัยศรีปทุม

ข้าพเจ้า (นาย/นาง/นางสาว) วิระชัย ศรีทัญชัย
 ตำแหน่ง ผู้ช่วยกรรมการฝ่าย ชื่อหน่วยงาน ฝ่ายพัฒนาระบบบริหารการงาน
 สถานที่ตั้ง อพตารักษ์นครราชสีมา จำกัด (มหาชน) ๕๕๐ ถนนเพลินจิต ปทุมธานี ๑๐๖๖๐
 โทรศัพท์ ๐๙๖-๑๙๒๒๔-๑๕ Email verachai.sirikhvuchai@kprgsri.com

ขอรับรองว่าได้นำผลงานทางวิชาการ/วิจัยเรื่อง/งานสร้างสรรค์ เรื่อง การพัฒนาระบบป้องกัน
 และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์
 ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ โดยมีซึ่งเป็นของ นาย กฤษ ศรีจินดี มาใช้ประโยชน์ในองค์กร/
 หน่วยงาน/กลุ่มของข้าพเจ้า โดยใช้ในระหว่างวันที่.....ถึงวันที่.....

ก่อให้เกิดผลดีในด้านต่อไปนี้ (ทำเครื่องหมาย ☒ เลือกได้มากกว่า ๑ ข้อ)

☒ การใช้ประโยชน์เชิงวิชาการ ☐ การใช้ประโยชน์เชิงสาธารณะ

☒ การใช้ประโยชน์เชิงนโยบาย ☐ การใช้ประโยชน์เชิงพาณิชย์

☐ การใช้ประโยชน์ทางอื่น

(โปรดระบุรายละเอียด).....

ข้าพเจ้าขอลงนาม ในหนังสือรับรองการนำไปใช้ประโยชน์ด้วยความจริงทุกประการ เพื่อเป็นหลักฐาน
 การประโยชน์จากผลงานวิจัยหรืองานสร้างสรรค์ ของ นาย กฤษ ศรีจินดี

ลงลายมือชื่อ.....

(นายวิระชัย ศรีทัญชัย)

วันที่...../...../.....



หนังสือรับรองการให้ประโยชน์ผลงานวิจัย
มหาวิทยาลัยศรีปทุม

ข้าพเจ้า (นาย/นาง/นางสาว) Mr. Aumnaj Kongjaroenthin
ตำแหน่ง General Manager ชื่อหน่วยงาน Taknet Systems (Thailand) Co., Ltd
สถานที่ตั้ง No. 43 Soi Romklao 44, Romklao Rd, Klongsamprawet, Latkrabang, Bangkok
โทรศัพท์ 0869052979 Email aumnaj@taknet.co.th

ขอรับรองว่าได้นำผลงานทางวิชาการ/วิจัยเรื่อง/งานสร้างสรรค์ เรื่อง การพัฒนาระบบป้องกัน
และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์
ตอบสนองต่อกับคุกคามแบบเรียลไทม์ โดยมีซึ่งเป็นของ นาย กฤษ ศรีเงินดี มาใช้ประโยชน์ในองค์กร/
หน่วยงาน/กลุ่มของข้าพเจ้า โดยใช้ในระหว่างวันที่ 22/May/2024 ถึงวันที่ 24/May/2024
ก่อให้เกิดผลดีในด้านต่อไปนี้ (ทำเครื่องหมาย ☒ เลือกได้มากกว่า 1 ข้อ)

- ☒ การใช้ประโยชน์เชิงวิชาการ ☒ การใช้ประโยชน์เชิงสาธารณะ
☒ การใช้ประโยชน์เชิงนโยบาย ☒ การใช้ประโยชน์เชิงพาณิชย์
☐ การใช้ประโยชน์ทางอื่น

(โปรดระบุรายละเอียด)

ข้าพเจ้าขอลงนาม ในหนังสือรับรองการนำไปใช้ประโยชน์ด้วยความจริงทุกประการ เพื่อเป็นหลักฐาน
การประโยชน์จากผลงานวิจัยหรืองานสร้างสรรค์ ของ นาย กฤษ ศรีเงินดี

ลงลายมือชื่อ Aumnaj K.
(Mr. Aumnaj Kongjaroenthin)
วันที่ 24 May 2024



หนังสือรับรองการใช้ประโยชน์ผลงานวิจัย

มหาวิทยาลัยศรีปทุม

ข้าพเจ้า (นาย/นาง/นางสาว) นาย บัณฑิต ปินนอมณี

ตำแหน่ง กรรมการบริษัท ชื่อบริษัท เอทีแอล ค้าค้า เทคโนโลยี จำกัด

สถานที่ตั้ง 388 อาคารเอกเจมทาวเวอร์ ถนนสุขุมวิท แขวงคลองเตย เขตคลองเตย กรุงเทพฯ 10110

โทรศัพท์ 0972380616 Email bundit.pinnomnace@gmail.com

ขอรับรองว่าได้นำผลงานทางวิชาการ/วิจัยเรื่อง/งานสร้างสรรค์ เรื่อง การพัฒนาระบบป้องกัน

และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์

ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ โดยมีซึ่งเป็นของ นาย กฤษ ศรีเงินดี มาใช้ประโยชน์ในองค์กร/

หน่วยงาน/กลุ่มของข้าพเจ้า โดยใช้ในระหว่างวันที่ 15/5/2567 ถึงวันที่ 24/5/2567 ก่อให้เกิดผล

ในด้านต่อไปนี้ (ทำเครื่องหมาย ☒ เลือกได้มากกว่า 1 ข้อ)

- ☐ การใช้ประโยชน์เชิงวิชาการ ☒ การใช้ประโยชน์เชิงสาธารณะ
☒ การใช้ประโยชน์เชิงนโยบาย ☒ การใช้ประโยชน์เชิงพาณิชย์
☐ การใช้ประโยชน์ทางอื่น

(โปรดระบุรายละเอียด).....

ข้าพเจ้าขอลงนาม ในหนังสือรับรองการนำไปใช้ประโยชน์ด้วยความจริงทุกประการ เพื่อเป็นหลักฐาน

การใช้ประโยชน์จากผลงานวิจัยหรืองานสร้างสรรค์ ของ นาย กฤษ ศรีเงินดี



ลงลายมือชื่อ กฤษ ศรีเงินดี
 (กฤษ ศรีเงินดี)
 วันที่ 24 / 5 / 2567



หนังสือรับรองการใช้ประโยชน์ผลงานวิจัย

มหาวิทยาลัยศรีปทุม

ข้าพเจ้า (นาย/นาง/นางสาว) สุชาติ ลิ้มล้ำม
 ตำแหน่ง คณบดีมหาวิทยาลัยราชภัฏวชิรเวศน์ ชื่อหน่วยงาน คณะวิทยาศาสตร์และเทคโนโลยี
 สถานที่ตั้ง มทว. รัชบุรีวชิ 39 ม.1 ต.คลองเตย อ.คลองหลวง จ.ปทุมธานี
 โทรศัพท์ 02-5494164 Email suchart-su@hotmail.com

ขอรับรองว่าได้นำผลงานทางวิชาการ/วิจัยเรื่อง/งานสร้างสรรค์ เรื่อง การพัฒนาระบบป้องกัน
 และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย โดยใช้เทคนิคการวิเคราะห์เหตุการณ์
 ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ โดยมีซึ่งเป็นของ นาย กลุข ศรีเงินดี มาใช้ประโยชน์องค์กร/
 หน่วยงาน/กลุ่มของข้าพเจ้า โดยใช้ในระหว่างวันที่ 25 พ.ค. 67 ถึงวันที่ 24 มิ.ย. 68
 ก่อให้เกิดผลดีในด้านต่อไปนี้ (ทำเครื่องหมาย ☒ เลือกได้มากกว่า 1 ข้อ)

- ☒ การใช้ประโยชน์เชิงวิชาการ ☐ การใช้ประโยชน์เชิงสาธารณะ
☒ การใช้ประโยชน์เชิงนโยบาย ☐ การใช้ประโยชน์เชิงพาณิชย์
☒ การใช้ประโยชน์ทางอื่น

(โปรดระบุรายละเอียด) ใช้ในงานประชุมของตึกใช้กับเครือข่าย
ระบบฐานข้อมูล

ข้าพเจ้าขอสงวนนาม ในหนังสือรับรองการนำไปใช้ประโยชน์ด้วยความจริงทุกประการ เพื่อเป็นหลักฐาน
 การประโยชน์จากผลงานวิจัยหรืองานสร้างสรรค์ ของ นาย กลุข ศรีเงินดี

ลงลายมือชื่อ

(นายสุชาติ ลิ้มล้ำม)
 วันที่ 25 พ.ค. 67



หนังสือรับรองการใช้ประโยชน์ผลงานวิจัย
มหาวิทยาลัยศรีปทุม

ข้าพเจ้า (นาย/นาง/นางสาว) วรวิทย์ กิ่งทอง
ตำแหน่ง Sr.Product ชื่อหน่วยงาน Control A solutions
สถานที่ตั้ง อาคาร ๖ ชั้น ๖๐๖
โทรศัพท์ ๐๘๖๙ ๗๖๖ ๖๕๑ Email wengmuw@outmail.com

ขอรับรองว่าได้นำผลงานทางวิชาการ/วิจัยเรื่อง/งานสร้างสรรค์ เรื่อง การพัฒนาระบบป้องกัน
และแจ้งเตือนข้อผิดพลาดทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์
ตอบสนองต่อข้อผิดพลาดแบบเรียลไทม์ โดยมีซึ่งเป็นของ นาย กฤษ ศรีเงินดี มาใช้ประโยชน์ในองค์กร/
หน่วยงาน/กลุ่มของข้าพเจ้า โดยใช้ในระหว่างวันที่ ๒๖/๕/๒๐๒๔ ถึงวันที่ ๒๗/๕/๒๐๒๔
ก่อให้เกิดผลดีในด้านต่อไปนี้ (ทำเครื่องหมาย ☒ เลือกได้มากกว่า ๑ ข้อ)

- ☐ การใช้ประโยชน์เชิงวิชาการ ☐ การใช้ประโยชน์เชิงสาธารณะ
☒ การใช้ประโยชน์เชิงนโยบาย ☒ การใช้ประโยชน์เชิงพาณิชย์
☐ การใช้ประโยชน์ทางอื่น

(โปรดระบุรายละเอียด).....

ข้าพเจ้าขอลงนาม ในหนังสือรับรองการนำไปใช้ประโยชน์ด้วยความจริงทุกประการ เพื่อเป็นหลักฐาน
การประโยชน์จากผลงานวิจัยหรืองานสร้างสรรค์ ของ นาย กฤษ ศรีเงินดี

ลงลายมือชื่อ วรวิทย์ กิ่งทอง
(
วันที่ ๒๗/๕/๒๕๖๗)



หนังสือรับรองการใช้ประโยชน์ผลงานวิจัย
มหาวิทยาลัยศรีปทุม

ข้าพเจ้า (นาย/นาง/นางสาว) ชัชวาลย์ เลี้ยงจรูญ
ตำแหน่ง นักวิจัยอาวุโสในตำแหน่งผู้บังคับบัญชาระดับสูง สำนักงานคณะกรรมการส่งเสริมการศึกษาเอกชน
สถานที่ตั้ง 319 ถนนจันทน์นอก แขวงจตุจักร เขตจตุจักร กรุงเทพมหานคร
โทรศัพท์ 061-7096969 Email chayawut.e@opec.go.th

ขอรับรองว่าได้นำผลงานทางวิชาการ/วิจัยเรื่อง/งานสร้างสรรค์ เรื่อง การพัฒนาระบบป้องกัน
และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่าย โดยใช้เทคนิคการวิเคราะห์เหตุการณ์
ตอบสนองต่อภัยคุกคามแบบเรียลไทม์ โดยมีซึ่งเป็นของ นาย กฤษ ศรีเงินดี มาใช้ประโยชน์ในองค์กร/
หน่วยงาน/กลุ่มของข้าพเจ้า โดยใช้ในระหว่างวันที่ 24 พฤศจิกายน 2561 ถึงวันที่

ก่อให้เกิดผลดีในด้านต่อไปนี้ (ทำเครื่องหมาย ☒ เลือกได้มากกว่า 1 ข้อ)

- ☐ การใช้ประโยชน์เชิงวิชาการ ☒ การใช้ประโยชน์เชิงสาธารณะ
☐ การใช้ประโยชน์เชิงนโยบาย ☒ การใช้ประโยชน์เชิงพาณิชย์
☐ การใช้ประโยชน์ทางอื่น

(โปรดระบุรายละเอียด)

ข้าพเจ้าขอลงนาม ในหนังสือรับรองการนำไปใช้ประโยชน์ด้วยความจริงทุกประการ เพื่อเป็นหลักฐาน
การประโยชน์จากผลงานวิจัยหรืองานสร้างสรรค์ ของ นาย กฤษ ศรีเงินดี

ลงลายมือชื่อ ชัชวาลย์
(นางชัชวาลย์ เลี้ยงจรูญ)
วันที่/...../.....

ประวัติย่อผู้วิจัย



ชื่อ – นามสกุล	กฤษ ศรีเงินดี
วัน เดือน ปี เกิด	15 พฤศจิกายน 2519
สถานที่เกิด	จังหวัดนครปฐม
วุฒิการศึกษา	- พ.ศ. 2546: วิทยาศาสตรบัณฑิต (อิเล็กทรอนิกส์) มหาวิทยาลัยราชภัฏนครปฐม. - พ.ศ. 2566: วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม.
ประสบการณ์ทำงาน	- พ.ศ. 2560 - ปัจจุบัน: ผู้จัดการฝ่ายการตลาดนวัตกรรม บริษัท พน์สออิเล็กทรอนิกส์ จำกัด - พ.ศ. 2559 - 2559: ผู้จัดการฝ่ายไอที บริษัท แกร็บแท็กซี่ (ประเทศไทย) จำกัด - พ.ศ. 2558 - 2559: ผู้จัดการฝ่ายบริการ (ไอที) บริษัท Singapore Telecommunications Limited, Comcentre, Orchard, Singapore. - พ.ศ. 2555 - 2558: ผู้ช่วยผู้จัดการฝ่ายปฏิบัติการด้านไอที บริษัท อาร์เอ็มเอ กรุ๊ป จำกัด - พ.ศ. 2554 - 2555: ผู้จัดการผลิตภัณฑ์อาวุโส บริษัท ดี ดิสทริบิวแอนด์ มาร์เก็ตติ้ง จำกัด
ที่อยู่ปัจจุบัน	429/41 แขวงบางมด เขตทุ่งครุ จังหวัดกรุงเทพมหานคร 10140

ผลงานทางวิชาการ

- [1] กฤษ ศรีเงินดี, ประสงค์ ปราณีตพลกรัง และสุรศักดิ์ มั่งสิงห์, “การพัฒนาระบบติดตาม เฝ้าระวัง และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคของการวิเคราะห์เหตุการณ์ตอบสนองแบบเรียลไทม์,” Rattanakosin Journal of Science and Technology (RJST), Vol.6, Issue 2, 2024.
- [2] Kit Sringendee, Prasong Praneetpolgrang and Surasak Mungsing, “Developing Proactive Cyber Threat Defense Systems on Server Computers Using Honeypot Techniques,” International Journal of Engineering Research & Technology (IJERT), Vol.13, Issue 06, 2024.