Rattanakosin Journal of Science and Technology: RJST
2024, Volume 6 Issue 2: 40-56
*Research Article*
*Online ISSN: 2673-0553*

# การพัฒนาระบบติดตาม เฝ้าระวัง และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคของการวิเคราะห์เหตุการณ์ตอบสนองแบบเรียลไทม์

# 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 ปราณีตพลกรัง[2] และ สุรศักดิ์ มังสิงห์[3]
[1*,2,3]หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
[1*]E-mail: kit.sringendee@gmail.com

**บทคัดย่อ**

การวิจัยครั้งนี้มีวัตถุประสงค์ เพื่อพัฒนาระบบที่สามารถแจ้งเตือนภัยคุกคามทางไซเบอร์ ประเภทการสุ่มหรือคาดเดาที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายหรือเซิร์ฟเวอร์ ที่มีให้บริการการเข้าถึงข้อมูลจากภายนอกองค์กร ทั้งนี้ ระบบที่พัฒนาขึ้นได้ทำการแจ้งเตือนให้ผู้ดูแลเครื่องเซิร์ฟเวอร์ด้วยเวลาที่ใกล้เคียงกับเวลาจริงหรือเรียลไทม์ เพื่อที่จะยับยั้งความเสียหายอันเกิดขึ้นกับเครื่องเซิร์ฟเวอร์ และกำกับดูแลได้อย่างต่อเนื่องหากมีการบุกรุกทางไซเบอร์ที่อาจเกิดขึ้นได้ในเวลาใด ๆ ผลการวิจัยพบว่า การโจมตีเครื่องเซิร์ฟเวอร์ประเภทการสุ่มหรือคาดเดา นั้น ผู้วิจัยใช้ระบบติดตาม เฝ้าระวัง และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองแบบเรียลไทม์ที่พัฒนาขึ้น สามารถวิเคราะห์ติดตามและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องเซิร์ฟเวอร์ ได้มีประสิทธิภาพอยู่ในระดับมากที่สุด ($\overline{X}$ = 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

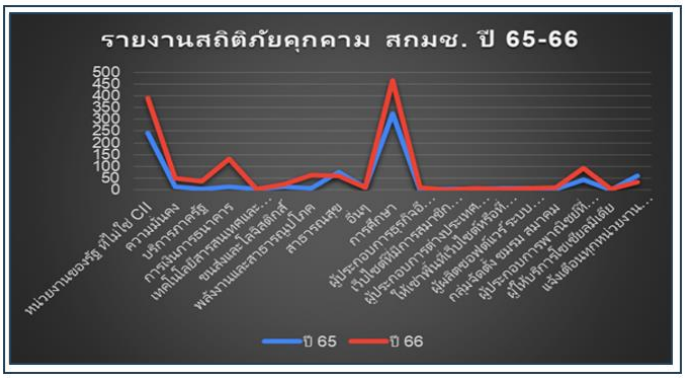
**Abstract**

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 ( $\overline{X}$ = 5.00)

**Keywords:** Alert, Cyber Threat, Server

## 1. บทนำ

ปัจจุบันมีการใช้บริการผ่านอินเทอร์เน็ตอย่างแพร่หลายอันส่งผลให้มีผู้ไม่หวังดีต้องการแสวงหาผลประโยชน์จากข้อมูลของผู้ใช้งานในระบบอินเทอร์เน็ต และต้องการเข้าถึงระบบแม่ข่ายของผู้ให้บริการ ซึ่งก่อให้เกิดความเสียหายแก่ผู้ให้บริการและผู้ใช้บริการ ตามสถิติของสานักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช) ดังรูปที่ 1 [1] พบว่าในปี 2565 มีรายงานภัยคุกคามทางไซเบอร์จำนวน 835 รายการ และในปี 2566 มีจำนวน 1,789 รายการ เพิ่มมากขึ้นถึง 214.2% แสดงให้เห็นว่าในปัจจุบันภัยคุกคามทางไซเบอร์มีอัตราการเติบโตอย่างต่อเนื่อง องค์กรต่าง ๆ ควรให้ความสำคัญกับภัยคุกคามทางไซเบอร์มากขึ้น




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

ปัจจุบันระบบการตรวจหา วิเคราะห์และตอบสนองต่อภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ (Security Information and Event Management: SIEM) เป็นทางออกหรือการแก้ปัญหาด้านความมั่นคง

ปลอดภัยไซเบอร์ โดยทำการรวบรวมข้อมูลเหตุการณ์จากแหล่งต่าง ๆ มาวิเคราะห์แบบทันทีทันใดหรือเรียลไทม์ (Real-Time) เพื่อตรวจจับกิจกรรมที่ผิดปกติ เมื่อนำ SIEM มาใช้ร่วมกับApplication Slack ที่เป็นแพลตฟอร์มการสื่อสารภายในองค์กรแล้วจะช่วยให้สมาชิกติดต่อสื่อสารกันได้ผ่านข้อความผ่านโทรศัพท์หรือการแชร์ไฟล์ได้สะดวกมากขึ้น ดังนั้นการนำ SIEM มาใช้จะช่วยในการตรวจสอบ วิเคราะห์และแจ้งเตือนภัยคุกคามทางไซเบอร์แบบเรียลไทม์จะช่วยเพิ่มประสิทธิภาพในการรักษาความมั่นปลอดภัยของคอมพิวเตอร์แม่ข่ายในองค์กรได้ดีมากยิ่งขึ้น

**2. วัตถุประสงค์ของการวิจัย**

1. เพื่อศึกษาวิเคราะห์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่าย

2. เพื่อพัฒนาระบบการแจ้งเตือนเมื่อเกิดภัยคุกคามแบบ Simple Brute Force Attacks อย่างเรียลไทม์

3. เพื่อทำการประเมินประสิทธิภาพการวิเคราะห์และแจ้งเตือนภัยคุกคามทางไซเบอร์แบบ Simple Brute Force Attacks อย่างเรียลไทม์

**3. กรอบแนวความคิดในการวิจัย**

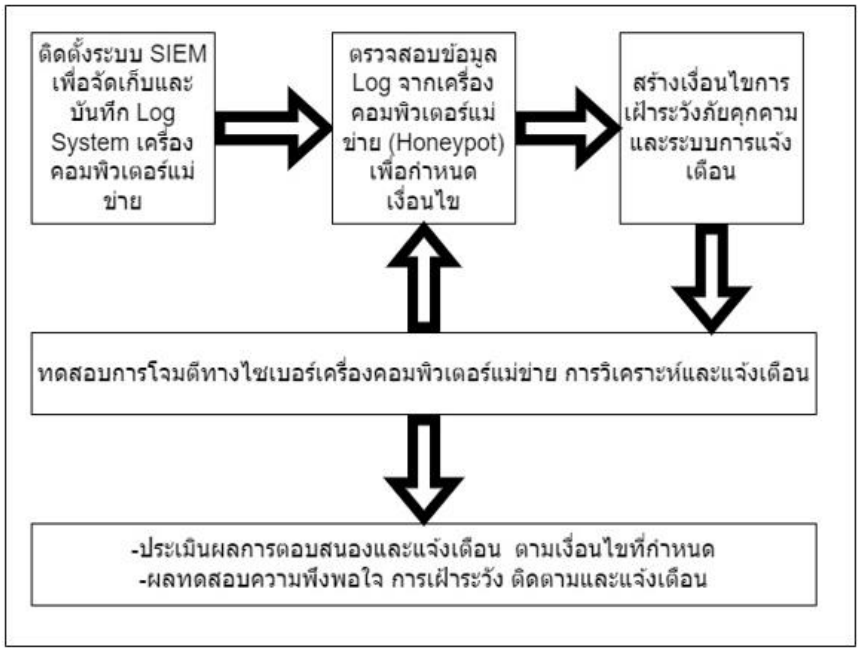
การวิจัยนี้ เป็นการพัฒนาระบบการแจ้งเตือนภัยคุกคามทางไซเบอร์ของเครื่องคอมพิวเตอร์แม่ข่ายโดยการโจมตีแบบ SSH Network Protocol แบบสุ่มรหัสผ่านผู้ดูแลระบบแบบเรียลไทม์ด้วยการกำหนดเงื่อนไขตามที่ผู้พัฒนาได้กำหนดและใช้ค่าเปรียบเทียบจาก MITRE ATT&CK Framework [2] โดยผู้วิจัยได้กำหนดกรอบแนวความคิดในการวิจัยดังรูปที่ 2 และมีขอบเขตของการวิจัย ดังนี้

1. การพัฒนาการวิเคราะห์ข้อมูลเหตุการณ์ (Log System) บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์เปรียบเทียบจาก 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

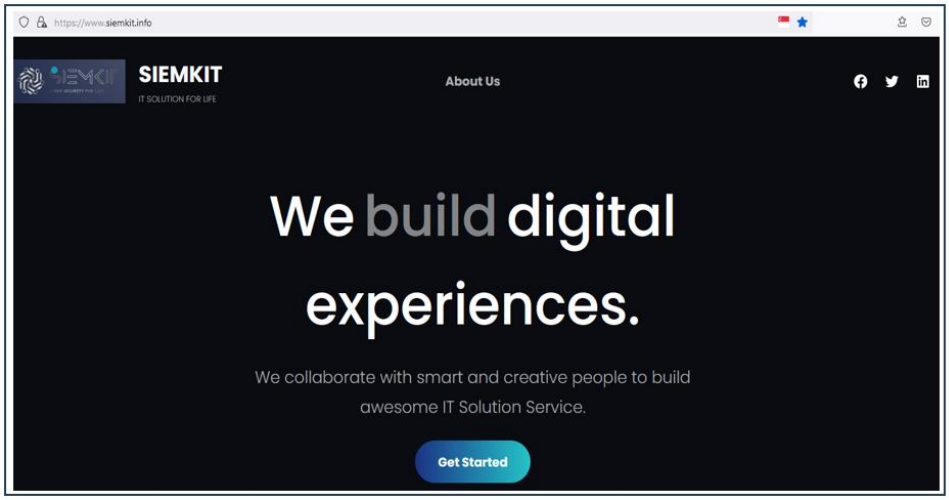
3. ใช้ภาษาไพทอน ในการอ่านข้อมูล Log ที่เขียนอยู่ในรูปแบบ JSON แล้วส่งข้อมูลมายังผู้ดูแลระบบ (Admin)

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

1. จัดเก็บข้อมูลการโจมตีแบบสุ่มรหัสผ่านทาง SSH port22 ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่าย

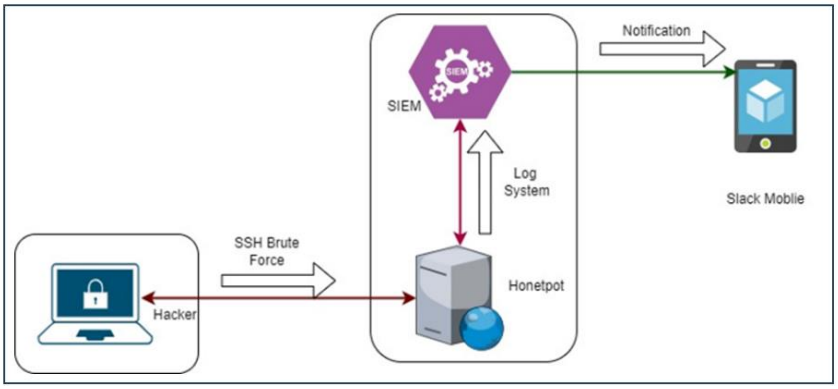
2. เปรียบเทียบกับเทคนิคการโจมตีในฐานข้อมูล MITRE ATT&CK Framework เพื่อทำเงื่อนไขการวิเคราะห์โจมตีเครื่องคอมพิวเตอร์แม่ข่ายและแจ้งเตือนผ่าน Application Slack

3. กำหนดรายละเอียดข้อมูลการแจ้งเตือนด้วยภาษาไพทอน (Python) ไปยัง Application Slack เพื่อให้ผู้ดูแลทราบถึงการแจ้งเตือน



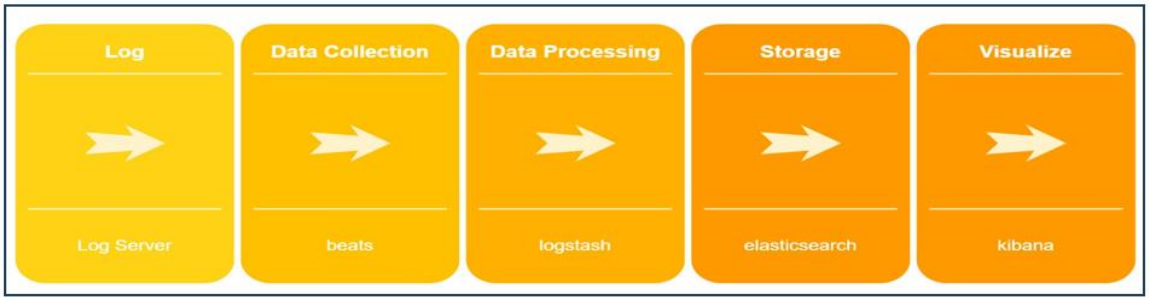

**รูปที่ 3** เครื่องคอมพิวเตอร์แม่ข่ายที่เป็นเหยื่อล่อ (Honeypot)

ขั้นตอนที่ 3 ประเมินประสิทธิภาพการวิเคราะห์และการแจ้งเตือนภัยคุกคามทางไซเบอร์แบบเรียลไทม์ โดยการทดสอบจำลองการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายโดยการคาดเดารหัสผ่าน ทาง SSH Port 22 เสมือนมีการโจมตีทางไซเบอร์ผ่านช่องทาง Internet จากนั้นเก็บผลระยะเวลาที่ใช้ในการวิเคราะห์และแจ้งเตือนเพื่อประเมินประสิทธิภาพการตอบสนองการโจมตี ที่เกิดขึ้นกับการเครื่องคอมพิวเตอร์แม่ข่าย ที่เกิดขึ้นตามกระบวนการทำงานที่ผู้วิจัยแสดง ดังรูปที่ 4



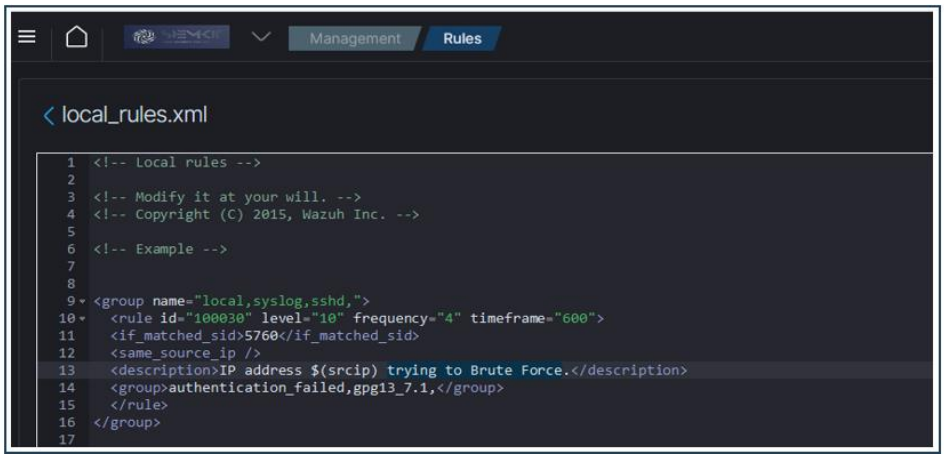

**รูปที่ 4** Flow System Diagram

งานวิจัยนี้ ผู้วิจัยได้พัฒนาระบบติดตาม เฝ้าระวัง และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองแบบเรียลไทม์ ทั้งนี้ได้นำระบบ SIEM ประเภทหนึ่งที่ชื่อ Wazuh เข้ามาใช้ในการจัดเก็บ Log จากเหตุการณ์การโจมตีเครื่องคอมพิวเตอร์แม่ข่าย โดย Wazuh Server ที่ทำงานร่วมกับ Elastic Stack เมื่อเกิดเหตุการณ์ขึ้นที่เครื่องคอมพิวเตอร์แม่ข่าย โปรแกรม Agent (bests) 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 ตรงกับกฎที่กำหนดไว้เมื่อก่อนหน้านี้ก็ให้วิเคราะห์แบบพยายามสุ่มหรือคาดเดา และกำหนด Rule ID ใหม่เป็นค่า 100030 จากนั้นก็นำค่า 100030 ไปกำหนดเงื่อนไขของการแจ้งเตือนไปยังผู้ดูแลระบบด้วย Application Slack ต่อไป ดังรูปที่ 6




**รูปที่ 6** แสดงกำหนดกฎเงื่อนไขใน Wazuh Server

เมื่อผู้วิจัย ได้ค่าของ Rule ID แล้วก็นำค่าที่ได้มาเป็นเงื่อนไขในการกำหนดการแจ้งเตือนผู้ดูแลระบบด้วย Application Slack ผ่าน API โดยกำหนด พารามิเตอร์ใน Wazuh Server ในส่วนของคำสั่ง Integrates โดยจะไปสั่งงานด้วยคำสั่งภาษาไพทอน ส่งรายละเอียดจาก Log ที่บันทึกในกฎ 100030 ไปยัง Slack API และแสดงค่าที่ 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>
```

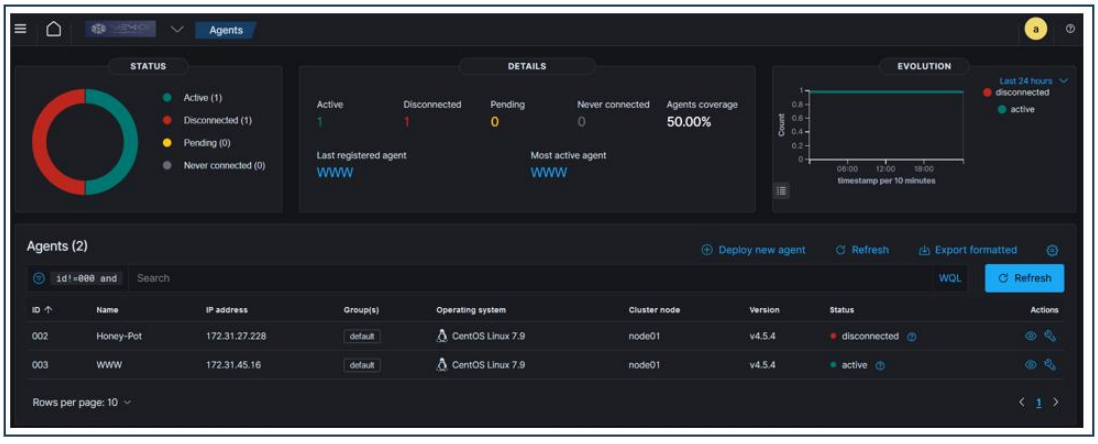
**รูปที่ 7** แสดงพารามิเตอร์เงื่อนไขการแจ้งเตือน Wazuh Server

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} _(Level {1})_".format(alert['rule']['id'], level),
    })

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

    return json.dumps(attach)
```

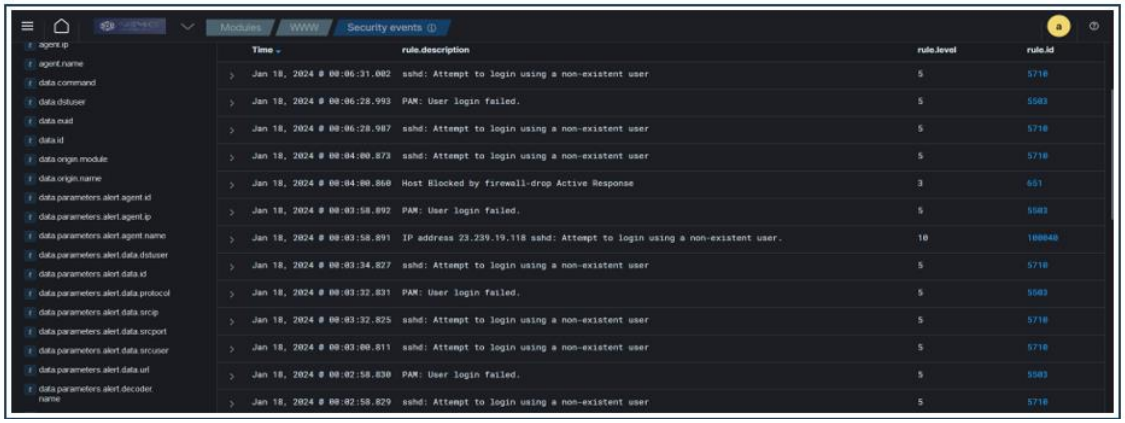
**รูปที่ 8** แสดงคำสั่งไพทอนรายงานการโจมตีไปยัง Slack API

1. ระบบ SIEM Open Source (Wazuh) เป็นแพลตฟอร์มรักษาความมั่นคงปลอดภัยโอเพนซอร์สที่มีความสามารถในด้านการจัดเก็บและรวบรวมเหตุการณ์ต่าง ๆ ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายจากการอ่านไฟล์ Log System ที่เกิดขึ้นในเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งโปรแกรม Agent ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์แม่ข่ายจะทำการอ่านและส่งข้อมูล Log มายังระบบ Wazuh Server เพื่อวิเคราะห์และแยกแยะข้อมูลออกเป็นส่วน ๆ เพื่อให้เข้าใจเหตุการณ์ที่เกิดขึ้น และรายละเอียดของเหตุการณ์ พร้อมทั้งเปรียบเทียบเหตุการณ์ที่เกิดขึ้นว่าเป็นภัยคุกคามกับ MITRE ATT&CK Framework หรือไม่ อีกทั้งสามารถนำค่าเปรียบเทียบไปตรวจสอบกับกฎที่กำหนด เพื่อดำเนินการสั่งชุดคำสั่งต่าง ๆ ได้ในเวลาเดียวกัน ซึ่งโดยแพลตฟอร์มแสดงการวิเคราะห์เหตุการณ์จาก Log System ที่เกิดขึ้นได้แบบเรียลไทม์และสร้างรายงานเพื่อใช้ในการสรุปเหตุการณ์ตามช่วงเวลาได้อีกด้วย ตัวอย่างแสดงแดชบอร์ดอินเทอร์เฟซของระบบ Wazuh Server ดังรูปที่ 9



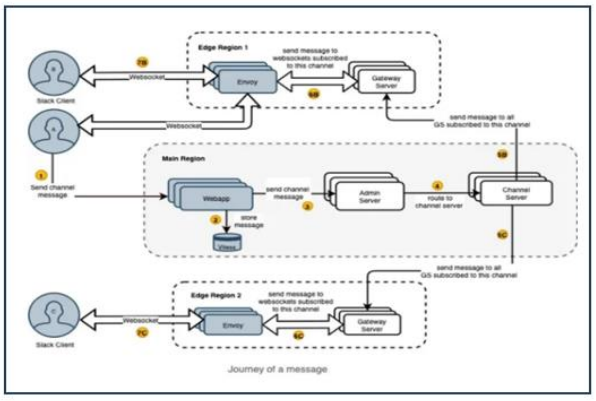

**รูปที่ 9** แสดงแดชบอร์ดอินเทอร์เฟซผู้ใช้งานระบบ SIEM

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




**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

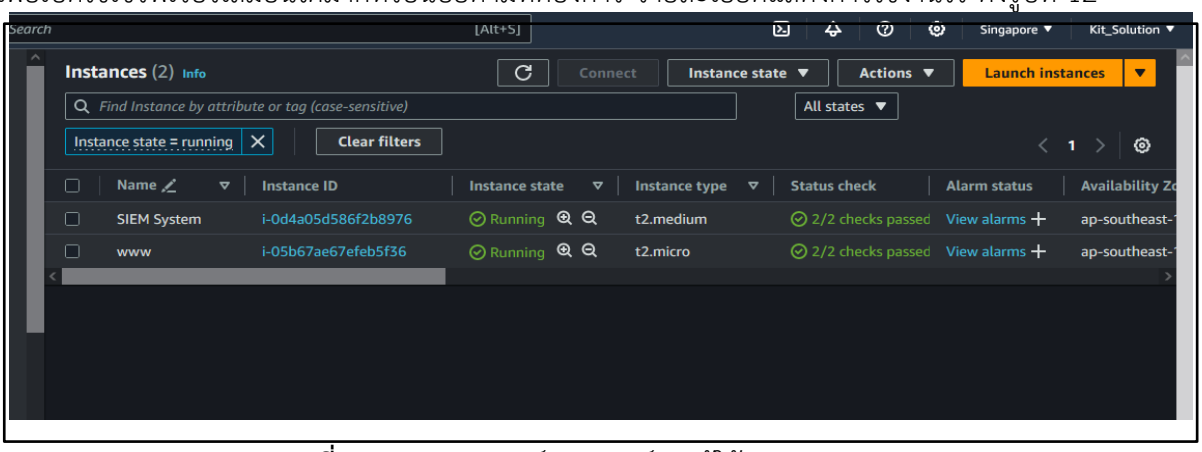



**รูปที่ 11** แสดง Data Flow Message (Slack. Engineering, 2566)

4. ระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย CentOS7 ใช้สำหรับเว็บเซิร์ฟเวอร์ ซึ่งมีหน้าที่เป็น Honeypot โดยระบบปฏิบัติการ CentOS7 ใช้สำหรับองค์กรที่เน้นเรื่องความเสถียรภาพ

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 ซึ่งมุ่งเป้าไปที่การทดสอบการเจาะข้อมูลขั้นสูง และการตรวจสอบความมั่นคงปลอดภัย การกำหนดค่า และระบบอัตโนมัติที่ช่วยให้ผู้ใช้มุ่งเน้นไปที่งานที่ต้องทำให้เสร็จ Kali Linux มีการดัดแปลงเฉพาะอุตสาหกรรม รวมถึงเครื่องมือหลายร้อยรายการที่มุ่งเป้าไปที่งานด้านความมั่นคงปลอดภัยของข้อมูลต่าง ๆ เช่น การทดสอบการเจาะข้อมูล การวิจัยความมั่นคงปลอดภัยนิติคอมพิวเตอร์ วิศวกรรมย้อนกลับ และการจัดการช่องโหว่

7. แบบประเมินประสิทธิภาพที่มีต่อการทำงานของระบบติดตาม เฝ้าระวัง และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองแบบเรียลไทม์ มีลักษณะเป็นแบบมาตราส่วนประมาณค่า 5 ระดับ (Rating Scale) แบบลิเคิร์ท (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

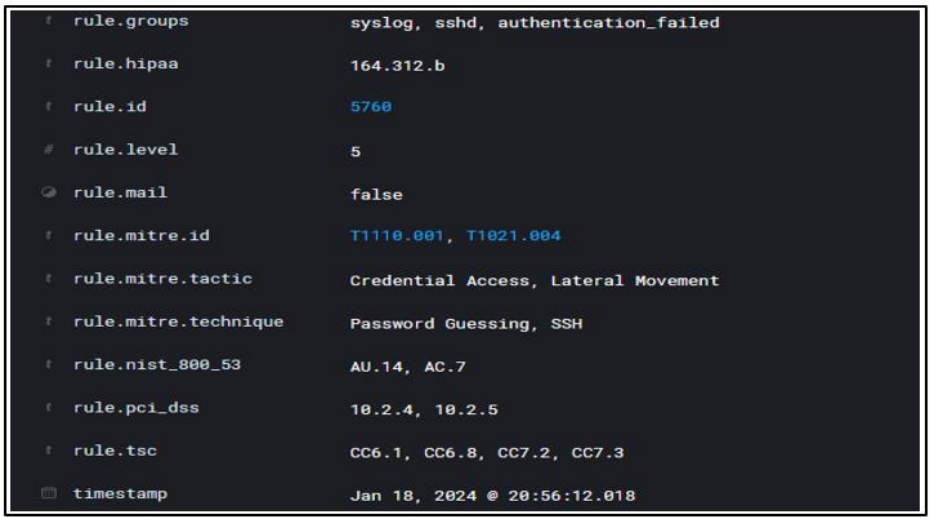
1. ผลศึกษาวิเคราะห์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับเครื่องเซิร์ฟเวอร์ คือ การมีความเสี่ยงทางไซเบอร์หรือการคาดการณ์ถึงการทำให้เกิดความเสียหายอันส่งผลกระทบต่อระบบคอมพิวเตอร์ ข้อมูล และอุปกรณ์คอมพิวเตอร์ต่าง ๆ เช่น การโจมตีด้วยไวรัสคอมพิวเตอร์ การบุกรุกเครือข่ายโดยที่ไม่ได้รับอนุญาต การขโมยข้อมูลส่วนบุคคล และการปฏิบัติการที่เกี่ยวกับความเป็นอันตรายของระบบเครือข่ายคอมพิวเตอร์ [5]

ภัยคุกคามทางไซเบอร์มีความหลากหลายและต้องการการระมัดระวังและการป้องกันที่เหมาะสม เพื่อป้องกันความเสี่ยงและการเข้าถึงข้อมูลที่ไม่เป็นไปตามกฎหมายหรือไม่ได้รับอนุญาต 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

จากผลการศึกษาวิเคราะห์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายในองค์กร ทำให้พบว่าการโจมตีแบบ Password Attacks หรือเรียกว่า Simple Brute Force Attacks เป็นการโจมตีที่พบมากที่สุดใน 7 ประเภทที่กล่าวมาข้างต้น ทำให้ผู้วิจัยได้ทำการวิจัยเพื่อทดสอบการติดตาม เฝ้าระวัง และแจ้งเตือน และนำไปสู่ผลการพัฒนาการแจ้งเตือนเมื่อเกิดภัยคุกคามแบบ Simple Brute Force Attacks อย่างเรียลไทม์

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




**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 วินาที จากไอพีต้นทางเดียวกัน 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,gpg13_7.1,</group>
  </rule>
</group>
```

**รูปที่ 14** เงื่อนไขเพื่อวิเคราะห์โจมตีแบบ Brute Force Attack

ผู้วิจัยนำค่า rule.id = 100030 เป็นข้อกำหนดการแจ้งเตือนไปที่ Application Slack ดังรูปที่ 15

```
<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>
```

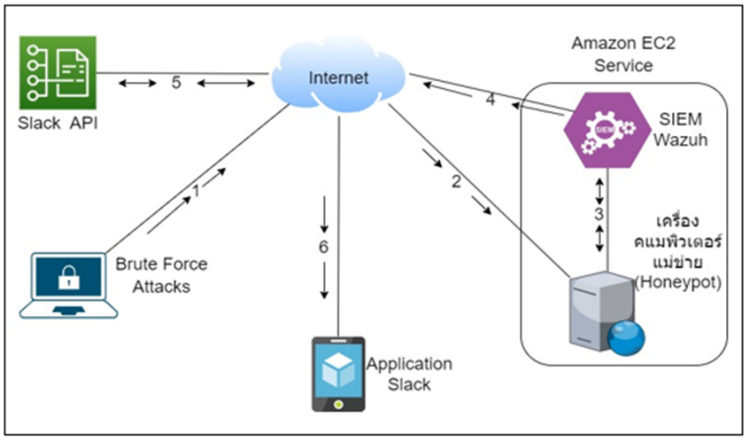
**รูปที่ 15** แสดงเงื่อนไขการแจ้งเตือน Brute Force Attack

เมื่อได้ทำการโจมตีครบจำนวนตรงตามกำหนดเงื่อนไขที่ไว้แล้ว ระบบ SIEM จะทำการบันทึกการโจมตีที่เกิดขึ้นไว้ในการบันทึกของระบบ SIEM ซึ่งจะทำให้ทราบว่ามีการพยายามโจมตีเครื่องคอมพิวเตอร์แม่ข่ายแบบ Simple Brute Force Attacks และแสดงหมายเลขกฎเป็น 100030 ดังรูปที่ 16

| | | | |
|---|---|---|---|
| › | Jan 18, 2024 @ 19:50:10.103 | IP address 58.11.20.33 trying to Brute Force. | 10 | 100030 |
| › | Jan 18, 2024 @ 19:50:10.101 | sshd: authentication failed. | 5 | 5760 |
| › | Jan 18, 2024 @ 19:50:08.367 | sshd: authentication failed. | 5 | 5760 |
| › | Jan 18, 2024 @ 19:50:08.122 | sshd: authentication failed. | 5 | 5760 |

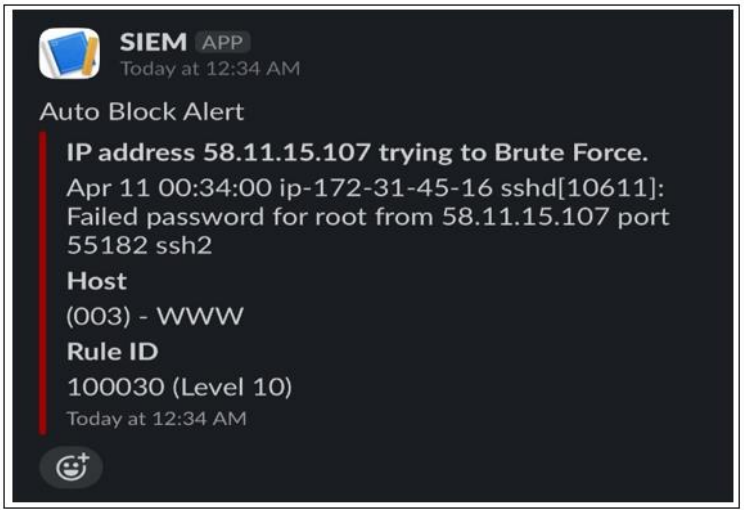
**รูปที่ 16** แสดงการวิเคราะห์โจมตีแบบ Brute Force Attack

ต่อมาจะส่งค่าพารามิเตอร์ที่ได้เฝ้าติดตามเครื่องคอมพิวเตอร์แม่ข่าย 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 ที่กำหนดขึ้นไปเปรียบเทียบกับเงื่อนไขที่อยู่ใน Integrates ในชุดคำสั่ง .XML ของระบบ SIEM ว่ามีข้อเงื่อนไขใด ๆ ที่ตรงกับ Rule ID = 100030 หรือไม่ หากพบว่าตรงกับ Rule ID = 100030 และค่าที่กำหนดไว้นั้น ให้ทำการส่งข้อความไปยัง API ตามช่องทางใด และพร้อมรายระเอียดจาก Log System ที่เก็บอยู่ในรูปแบบ JSON โดยการใช้ชุดคำสั่งไพทอนเรียกค่าต้องการส่งไปยังผู้ดูแลระบบเครื่องคอมพิวเตอร์แม่ข่าย ให้ทราบถึงภัยคุกคามที่เกิดขึ้น และตรวจสอบและดำเนินการป้องกันหรือยับยั้งต่อไป ดังรูปที่ 18




**รูปที่ 18** แสดงการแจ้งเตือนผ่าน Application Slack

3. ผลการประเมินประสิทธิภาพการวิเคราะห์และแจ้งเตือนภัยคุกคามทางไซเบอร์แบบเรียลไทม์ โดยนำระยะเวลาที่ใช้ในการวิเคราะห์และการแจ้งเตือนมาหาค่าเฉลี่ย ($\overline{X}$) และการทดสอบการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายและระยะที่ใช้ในการแจ้งเตือนผ่าน Application Slack เปรียบเทียบกับการโดนโจมตีแบบ Brute Force Attack ที่ถูกบันทึกลงไปในระบบ SIEM มีดังนี้

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

ระยะเวลาการวิเคราะห์หรือแจ้งเตือน 1 วินาที – 5 วินาที หมายถึงอยู่ในระดับ 5

ระยะเวลาการวิเคราะห์หรือแจ้งเตือน 6 วินาที – 10 วินาที หมายถึงอยู่ในระดับ 4

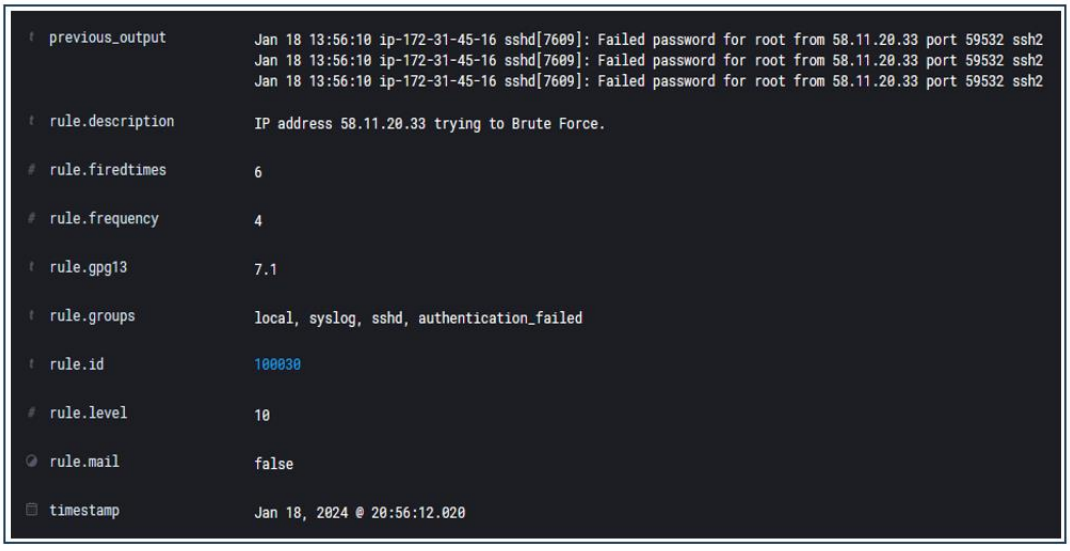
ระยะเวลาการวิเคราะห์หรือแจ้งเตือน 11 วินาที – 15 วินาที หมายถึงอยู่ในระดับ 3

ระยะเวลาการวิเคราะห์หรือแจ้งเตือน 16 วินาที – 20 วินาที หมายถึงอยู่ในระดับ 2

ระยะเวลาการวิเคราะห์หรือแจ้งเตือน 21 วินาที – 25 วินาที หมายถึงอยู่ในระดับ 1

ผลการทดสอบระบบการวิเคราะห์และการแจ้งเตือนเครื่องคอมพิวเตอร์แม่ข่าย จะพบว่าระบบ SIEM ได้ทำการวิเคราะห์และบันทึกการโจมตีที่ตรงตามเงื่อนไขกำหนด ผู้วิจัยนำเวลาเริ่มโจมตีมาเปรียบเทียบกับเวลาที่ทำการแจ้งเตือน ซึ่งเวลาเป็นการบันทึกด้วยระบบ SIEM อัตโนมัติ รายละเอียดดังรูปที่ 19 และ 20


**รูปที่ 19** แสดงผลการวิเคราะห์และบันทึกการโจมตี




**รูปที่ 20** แสดงรายละเอียดการวิเคราะห์และรูปแบบการโจมตี

เมื่อมีการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายที่เกิดขึ้น ตรงตามกฎที่ผู้วิจัยกำหนดไว้ ดังรูปที่ 19 และรูปที่ 20 จะพบว่ามีการบันทึกเวลากิจกรรมที่เกิดขึ้นตามอ้างอิงจากระบบ SIEM ลงบันทึกไปใน Log System ของระบบ SIEM เพื่อเป็นการยืนยันเหตุการณ์ที่เกิดขึ้น ณ ขณะเกิดเหตุการณ์ ตั้งแต่เริ่มจนถึงจุดสิ้นสุด ตรงตามกฎเงื่อนไขที่กำหนด จึงนำค่ามาคำนวณระยะเวลาที่ใช้ในการวิเคราะห์เพื่อระบุภัยคุกคามที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายและการแจ้งเตือนภัยคุกคามไปยัง Application Slack ที่ตรงตามชุดคำสั่งสอดคล้องกับเงื่อนไขที่ผู้วิจัยได้กำหนดไว้ก่อนแล้วนั้น โดยการทดสอบเพื่อแสดงการค่าประสิทธิภาพของการวิเคราะห์หรือแจ้งเตือน 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** | $\overline{X}$ |
| **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 ในช่วงระยะเวลาการใส่รหัสผ่านที่ไม่ถูกต้องให้จำนวนห่างกันในการทดสอบชุดที่ 1, 2, 4 และติด ๆ กัน ชุดที่ 3, 5 นั้น เพื่อทดสอบการประมวลผลการตรวจจับที่เป็นไปตามเงื่อนไขที่ได้กำหนดไว้ในค่า .XML ไฟล์ ซึ่งถ้าหากเป็นบุคคลใส่รหัสผิดก็จะต้องมีการทบทวนรหัสผ่านก่อนที่จะใส่ในครั้งต่อไป ซึ่งต่างจากการ Brute Force Attack ที่พยายามให้เข้าเครื่องคอมพิวเตอร์แม่ข่ายให้เร็วที่สุด และใช้เวลาน้อยที่สุด

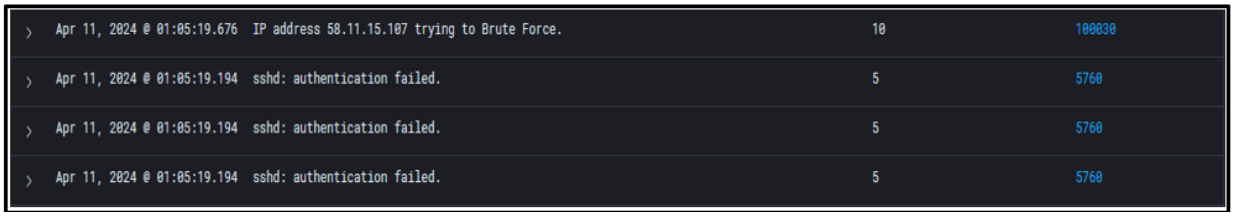
**ตารางที่ 2** ผลระยะเวลาการแจ้งเตือนแบบเรียลไทม์

| **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** | $\overline{X}$ |
| **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 |

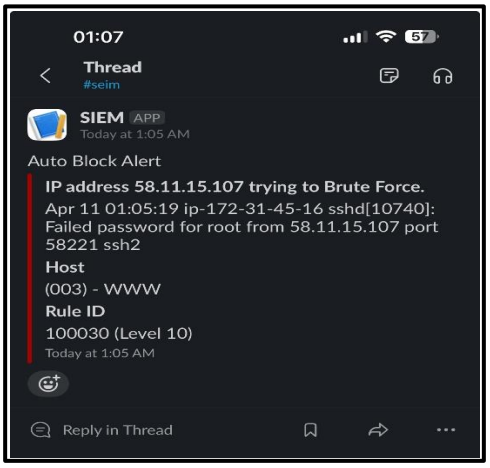
ผลการทดสอบตารางที่ 2 เมื่อตรวจจับ Rule ID = 100030 ในเวลาที่สิ้นสุดการ Brute Force Attack ระบบ SIEM ได้มีการแจ้งเตือนไปยังผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายผ่าน Slack Application โดยเปรียบเวลาที่แสดงว่ามีการตรวจจับการ Brute Force Attack โดยใช้ Rule ID = 100030 ในการส่งค่าการแจ้งเตือน โดยเปรียบเทียบกับเวลาได้ข้อความมีเวลาเดียวกันกับเมื่อ SIEM แสดง Log ที่เป็น Rule ID = 100030

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


**รูปที่ 21** แสดง Brute Force Attack แบบเว้นระยะเวลา




**รูปที่ 22** แสดง Brute Force Attack แบบระยะเวลาติดกัน




**รูปที่ 23** แสดงการแจ้งเตือน Brute Force Attack

## 6. อภิปรายผลและข้อเสนอแนะ

1. ในงานวิจัยนี้เป็นการวิเคราะห์ภัยคุกคามที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งผู้วิจัยได้ทำการจัดเก็บ Log System จากเครื่องคอมพิวเตอร์แม่ข่ายที่เป็นเหยื่อล่อ นำมาวิเคราะห์การโจมตี และกำหนดกฎ

เงื่อนไขเพิ่มเติม เพื่อใช้นำการติดตาม เฝ้าระวังและแจ้งเตือน ภัยคุกคามแบบ Brute Force โดยเมื่อเกิดเหตุการณ์ภัยคุกคามที่เครื่องคอมพิวเตอร์แม่ข่ายตรงกับค่าพารามิเตอร์ทั้งกำหนดไว้ ก็จะทำให้ทราบถึงภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายได้โดยง่าย เพราะเทคนิคการโจมตีทางไซเบอร์ได้มีการตั้งค่าเงื่อนไขพร้อมการแจ้งเตือนไปยังผู้ดูแลระบบเครื่องคอมพิวเตอร์แม่ข่าย และยังสามารถส่งข้อมูลที่จำเป็นใช้ในการแจ้งเตือนไปได้ภายในครั้งเดียว และลดระยะเวลาของการตรวจสอบเครื่องคอมพิวเตอร์แม่ข่ายไปพร้อม ๆ กันได้

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

3. การประเมินประสิทธิภาพการวิเคราะห์และแจ้งเตือนภัยคุกคามแบบเรียลไทม์ ซึ่งงานวิจัยนี้ได้สะท้อนผลการเปรียบเทียบระยะเวลาการแจ้งเตือนกับการบันทึกข้อมูลภัยคุกคามที่เกิดนั้น จะมีค่าระยะเวลาตามผลการวิเคราะห์ภัยคุกคามทางไซเบอร์ได้ผลค่าประสิทธิภาพในระดับมากที่สุด ($\overline{X}$ = 5.00) และค่าการแจ้งเตือนมีค่าประสิทธิภาพอยู่ในระดับมากที่สุด ($\overline{X}$ = 5.00) เช่นกัน ซึ่งเป็นผลดีในการนำเอาระบบนี้ไปใช้งานจริง หากเกิดภัยคุกคามทางไวเบอร์ตามที่ได้กำหนดการเฝ้าระวังไว้ อย่างไรก็ตามค่าความรวดเร็วนี้อาจจะต้องอาศัยประสิทธิภาพของระบบเครือข่ายคอมพิวเตอร์หรืออินเทอร์เน็ตที่องค์กรเชื่อมต่ออยู่ด้วย นอกจากนั้นการแจ้งเตือนไปยัง Application Slack นั้น ยังไม่มีค่าใช้จ่ายใด ๆ สำหรับการเรียกใช้งานผ่าน API และใช้งานได้ทั้งบนเครื่องโมไบล์ และคอมพิวเตอร์ส่วนบุคคล ซึ่งเป็นการเพิ่มความสะดวกและคล่องตัวให้กับผู้ดูแลระบบเครื่องคอมพิวเตอร์แม่ข่ายให้ติดตาม เฝ้าระวังการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายได้ตลอดเวลา ในทุกที่ ๆ สามารถเข้าถึงอินเตอร์เน็ต หากแม้ว่าไม่ได้อยู่กับเครื่องคอมพิวเตอร์แม่ข่ายนั้น ๆ อีกทั้งยังประหยัดค่าใช้จ่ายในการพัฒนาแอปพลิเคชันเพื่อใช้สำหรับการแจ้งเตือนอีกด้วย

อย่างไรก็ตาม การศึกษาวิจัย การพัฒนาระบบติดตาม เฝ้าระวัง และแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองแบบเรียลไทม์ ผู้วิจัยมีข้อเสนอแนะจากการศึกษาครั้งนี้ดังนี้

1. ข้อเสนอแนะในการนำผลการวิจัยไปใช้งานจริง ซึ่งจากระบบที่ได้มีการพัฒนาขึ้นนี้ สามารถนำไปปรับใช้กับองค์กรที่ต้องการรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการแบบเข้าถึงจากภายนอกองค์กรให้มีการแจ้งเตือนภัยคุกคามทางไซเบอร์ไปยังผู้ดูและระบบอันเป็นการยับยังการโจมตีทางไซเบอร์ได้ อีกทั้งเหมือนเป็นการพัฒนาระบบแบบโอเพนซอร์ส (Open Source) ที่ไม่ได้มีค่าใช้จ่ายใด ๆ

ในด้านค่าลิขสิทธิ์ (License) ยิ่งทำให้นำไปใช้ได้อย่างง่าย หากองค์กรนั้น ๆ มีข้อจำกัดด้านงบประมาณสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น สถาบันการศึกษา วิสาหกิจขนาดกลางและขนาดย่อม (SME) องค์กรไม่หวังผลกำไรต่าง ๆ และหน่วยงานภาครัฐ

2. ข้อเสนอแนะในการวิจัยครั้งต่อไป จากการวิจัยนี้ยังคงเป็นการวิจัยการโจมตีทางไซเบอร์แบบ Brute Force Attack เพียงอย่างเดียวอาจจะนำระบบ SIEM [8] นี้ไปพัฒนาต่อเรื่องการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายในแบบอื่น เช่น การโจมตีด้วย แรนซัมแวร์ มัลแวร์ การโจมตีแบบ DDoS เนื่องจากการทำงานของระบบ SIEM จะอ่านข้อมูลจาก Log System ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่าย หากระบบ SIEM อ่านค่ากิจกรรมที่เกิดขึ้นอันเป็นผลที่น่าสงสัยหรือไม่ปกติ ก็สามารถใช้ 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). ทำไมต้องลิเคิร์ต?. วารสารนวัตกรรมและการจัดการศูนย์ส่งเสริมและพัฒนางานวิจัย มหาวิทยาลัยศรีปทุม.

[5] ปรเมศวร์ กุมารบุญ. (2561). การส่งเสริมการศึกษาในวิชาอาชญากรรมไซเบอร์. กรุงเทพฯ: วารสารวิชาการอาชญาวิทยาและนิติวิทยาศาสตร์ 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] ธริช พงษ์รชนี. (2562). ระบบเฝ้าระวังและตรวจจับภัยคุกคามเว็บ เซิร์ฟเวอร์ Mini SOC Web Server. กรุงเทพฯ: มหาวิทยาลัยเทคโนโลยีมหานคร.

[10] กิตติภณ พละการ กิตติภพ พละการ สมชาย ประสิทธิ์จูตระกูล และสุกรี สินธุภิญโญ. (2561). Python 101. 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.