**รายงานสรุปผลการปฏิบัติงาน  
 ศูนย์เฝ้าระวังความปลอดภัยระบบคอมพิวเตอร์ และสารสนเทศ**

**(Security Operation Center)**

**ประจำเดือน มีนาคม 2565**

**บริษัท หลักทรัพย์จัดการกองทุน เอ็กซ์สปริง จำกัด**

**ประวัติการแก้ไขเอกสาร**

| **เวอร์ชัน** | **รายละเอียด** | **ผู้จัดทำ** | **วันที่อนุมัติ** |
| --- | --- | --- | --- |
| 1.0 | จัดทำร่างเอกสาร | ศูนย์ SOC | 1 กันยายน 2562 |
| 1.1 | จัดทำภาคผนวก | ศูนย์ SOC | 10 พฤศจิกายน 2563 |

**สารบัญ**

**หัวข้อ หน้า**

[หลักการและเหตุผล 4](#_Toc81248645)

[วัตถุประสงค์ 4](#_Toc81248646)

[บทสรุปสำหรับผู้บริหาร 5](#_Toc81248647)

[ภาพรวมของการเฝ้าระวังเหตุการณ์ด้านความปลอดภัย (Security Incident) 5](#_Toc81248648)

[สรุปจำนวนอุปกรณ์ที่ส่ง Log 6](#_Toc81248649)

[สรุปค่าเฉลี่ยจำนวน Log 6](#_Toc81248650)

[ภาคผนวก 7](#_Toc81248651)

**รายงานสรุปผลการดำเนินงานของศูนย์เฝ้าระวังความปลอดภัยระบบคอมพิวเตอร์ และสารสนเทศ**

**ประจำเดือน** **มีนาคม 2565**

**เสนอ**

**บริษัท หลักทรัพย์จัดการกองทุน เอ็กซ์สปริง จำกัด**

**จัดทำโดย บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน)**

## หลักการและเหตุผล

ในปัจจุบันหน่วยงานหรือองค์กรต่าง ๆ มีการนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ร่วมกับระบบงานต่าง ๆ อย่างแพร่หลาย เพื่อลดระยะเวลา เพิ่มประสิทธิภาพในการปฏิบัติงาน หรือแม้แต่การเสริมสร้างภาพลักษณ์ขององค์กร แก่ผู้ใช้บริการ เช่น การจัดทำเว็บไซต์ของหน่วยงาน เป็นต้น เครื่องให้บริการ (Server) อุปกรณ์ระบบเครือข่าย (Network) และระบบปฏิบัติการ (Operating System) เป็นองค์ประกอบที่สำคัญที่จะทำให้ระบบสารสนเทศสามารถให้บริการแก่ผู้ใช้บริการ อย่างไรก็ตาม เพื่อให้ระบบสารสนเทศสามารถให้บริการได้อย่างมีประสิทธิภาพ สิ่งที่สำคัญที่องค์กรจะขาดไม่ได้ คือ เจ้าหน้าที่ดูแลระบบสารสนเทศที่มีความเชี่ยวชาญในระบบสารสนเทศ มีความรู้ ความเข้าใจทั้งในเรื่องความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และ การแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้นในสถานการณ์เฉพาะหน้าในระบบงาน ที่ให้บริการแก่สาธารณะ หรือบุคลากรขององค์กร ในการให้บริการของระบบงานนั้น อาจมีกลุ่มคน ผู้ไม่ประสงค์ดีปะปน เข้ามาใช้บริการกับผู้ใช้งานทั่วไป เป็นเหตุให้ระบบเกิดความล่าช้า หรือไม่สามารถให้บริการแก่ผู้ใช้บริการได้อย่างมีประสิทธิภาพ ไปจนถึงการจารกรรมข้อมูล ซึ่งอาจจะก่อให้เกิดความเสียหายที่อาจจะประเมินมูลค่าไม่ได้

โดยการป้องกันเหตุการณ์เหล่านี้ จำเป็นจะต้องได้รับความร่วมมือหลาย ๆ ส่วน ไม่ว่าจะเป็นเจ้าของระบบงานนั้น ๆ ไปจนถึงผู้ให้บริการ ในการให้ความร่วมมือเพื่อป้องกันเหตุการณ์ที่อาจจะเกิดขึ้นและตรวจสอบเมื่อมีเหตุการณ์เกิดขึ้นแล้ว พร้อมด้วยความที่บุคลากรทางด้านเทคโนโลยีสารสนเทศของหน่วยงานนั้น อาจจะมีความตระหนักรู้ทางด้านความมั่นคงปลอดภัยสารสนเทศไม่เพียงพอ จึงมีความจำเป็นที่จะต้องมีหน่วยงานที่จะสามารถประสานงาน ให้ความรู้ และช่วยเสริมสร้างให้ระบบงาน บุคลากร ไปจนถึงภาพรวมของหน่วยงาน มีความมั่นคงปลอดภัยสารสนเทศ ที่เพิ่มมากขึ้น โดยอ้างอิงมาตรฐานสากลเพื่อให้มีความน่าเชื่อถือ และสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศของหน่วยงานให้ยั่งยืนต่อไป

## วัตถุประสงค์

1. เพื่อให้มั่นใจว่าเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น จะได้รับการเฝ้าระวัง และแจ้งเตือนได้อย่างมีประสิทธิภาพ ตรงตามขอบเขตการดำเนินงานที่บริษัทฯ ได้รับมอบหมายภายในสัญญาภายใต้โครงการฯ
2. เพื่อปฏิบัติ และดำเนินงานได้อย่างถูกต้องครบถ้วนตามขอบเขตของข้อกำหนดในโครงการฯ

## บทสรุปสำหรับผู้บริหาร

บริษัทฯ ได้สรุปเหตุการณ์การด้านความมั่นคงปลอดภัยระบบคอมพิวเตอร์ และสารสนเทศที่เกิดขึ้นในเดือนมีนาคม 2565 โดยมีรายละเอียดดังนี้

### ภาพรวมของการเฝ้าระวังเหตุการณ์ด้านความปลอดภัย (Security Incident)

จากผลการเฝ้าระวังประจำเดือนมีนาคม 2565 ตรวจพบเหตุการณ์ที่สำคัญ ดังรายละเอียด ต่อไปนี้

| **ลำดับ** | **ชื่อหน่วยงาน** | **จำนวนเหตุการณ์** | **CRITICAL** | **HIGH** | **MEDIUM** | **LOW** |
| --- | --- | --- | --- | --- | --- | --- |
| 1. | บริษัท หลักทรัพย์จัดการกองทุน เอ็กซ์สปริง จำกัด | 6 | 0 | 0 | 6 | 0 |

มีเหตุการณ์ที่น่าสนใจดังนี้

1. ตรวจพบเหตุการณ์ Brute Force Login Failed คือเหตุการณ์การพยายามเข้าสู่ระบบ แต่เข้าสู่ระบบไม่สำเร็จเป็นจำนวนมากโดยใช้ Username และ IP เดียวกัน ทำให้เกิดความเสี่ยงในการที่ผู้โจมตีจะค้นพบรหัสผ่านที่ถูกต้องและสามารถใช้ในการเข้าสู่ระบบได้สำเร็จ รวมไปถึงหากมีการพยายามเข้าสู่ระบบเป็นจำนวนมากอาจส่งผลกระทบให้ทรัพยากรของระบบถูกใช้งานเกินความจำเป็นซึ่งอาจนำไปสู่การทำงานหนักของระบบจนไม่สามารถให้บริการได้ชั่วคราว เหตุการณ์ดังกล่าวอาจเกิดจากการใช้งานแอพพลิเคชั่นที่ผิดพลาดทำให้เกิดการ Login Failed อยู่ที่เครื่องเป็นจำนวนมาก

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Source IP | Source Geolocation | Source User | Destination IP | Time |
| 192.168.106.31 | None | SanhapojA | 203.150.51.49 | 2022-03-03 16:55:03 |

**คำแนะนำ**

• ดำเนินการตรวจสอบว่า พฤติกรรมดังกล่าวเป็นการใช้งานปกติหรือไม่ (เช่น เป็นพฤติกรรมที่พนักงานภายในองค์กรทำการเข้าสู่ระบบล้มเหลว หรือเป็นการ Config ระบบผิดพลาดหรือไม่)
  
• หากพบว่าเป็นการโจมตี ให้พิจารณาทำการปรับแต่งการตั้งค่าการใช้งาน เพื่อหยุดเหตุการณ์ดังกล่าว (เช่น ทำการ Disable ชื่อผู้ใช้ที่ถูกโจมตีชั่วคราว)
  
• หากพบว่าเป็นการโจมตี ให้ทำการระงับการสื่อการกับหมายเลข IP ของผู้บุกรุกทันที (เช่น การควบคุม Traffic บน Firewall)
  
• กำหนดนโยบายของการใช้รหัสผ่านให้มีความแข็งแรงและปลอดภัย (เช่น ความยาวของรหัสผ่านอย่างน้อย 8 ตัวอักษร, ประกอบไปด้วยตัวอักษรพิมพ์ใหญ่, ประกอบไปด้วยตัวเลขและอักขระพิเศษ, ยากต่อการคาดเดา, การเปลี่ยนรหัสผ่านทุกๆ 3 เดือน)
  
• ไม่ควรอนุญาตให้ Default Username เช่น root หรือ administrator หรือ guest สามารถเข้าสู่ระบบจากระยะไกลได้ (แนะนำให้สร้าง Username ใหม่ที่อาจมีระดับสิทธ์เท่ากันมาใช้งานแทน)
  
• หากมีการเปิดให้บริการและมีความจำเป็นต้องใช้งานภายใน ให้พิจารณาเปิดการเข้าถึงเฉพาะ User ที่ได้รับอนุญาต หรือทำการต่อ VPN ก่อนเข้าถึงบริการส่วนตัว
  
• ทำการเปลี่ยนหมายเลข Port ที่ใช้สำหรับการเข้าสู่ระบบจากค่าเริ่มต้นให้เป็นเลขอื่น
  
• ควรมีการพิจารณา Update Patch/Hotfix ของ Software ที่เปิดให้บริการอยู่เสมอ เพื่อลดความเสี่ยงของการโจมตีจากช่องโหว่ต่าง ๆ

1. ตรวจพบเหตุการณ์ Inbound Communication With Blacklist IP Address เป็นเหตุการณ์ที่อุปกรณ์ภายนอกที่เป็น IP อันตราย ( Blacklist IP ) ทำการเชื่อมต่อเข้ามายังเครื่องภายในองค์กร

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Source IP | Source Geolocation | Destination IP | Port | Event Subtype | Time |
| 64.62.197.182 | None | 203.150.51.55 | 443 | pass | 2022-03-25 11:44:47 |
| 194.31.98.144 | None | 203.150.51.55 | 81 | pass | 2022-03-21 11:18:38 |
| 141.98.10.60 | None | 203.150.51.55 | 81 | pass | 2022-03-05 02:34:55 |
| 167.248.133.120 | None | 203.151.80.103 | 443 | pass | 2022-03-02 14:45:55 |
| 118.123.105.68 | None | 203.150.51.55 | 443 | pass | 2022-03-12 13:28:04 |

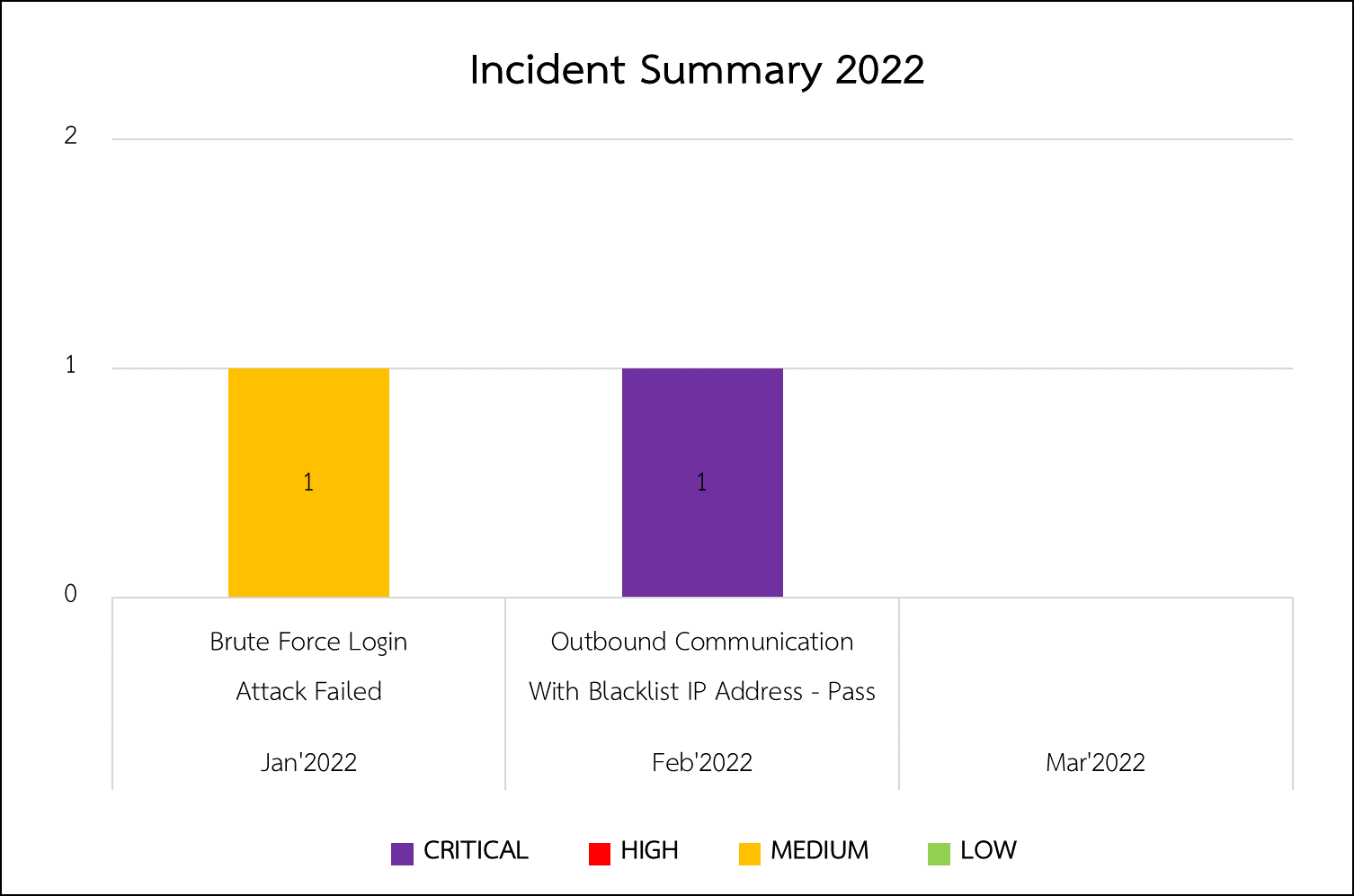
**คำแนะนำ**

• ดำเนินการตรวจสอบเครื่องภายในองค์การที่มีการเชื่อมต่อไปยังอุปกรณ์จากภายนอกที่เป็นอันตราย ( Blacklist IP ) เนื่องจากเครื่องเป้าหมายอาจจะติด Malware หลังจากมีการเชื่อมต่อไปยัง IP อันตราย ( Blacklist IP )
  
• ทำการ Full Scan เพื่อตรวจสอบว่าเครื่องเป้าหมายถูกติดตั้ง Malware ไว้หรือไม่และทำ Policy Firewall ไม่ให้มีการติดต่อกันของ IP ต้นทางที่เป็นอันตรายและ IP ปลายทางที่เป็นเครื่องภายในองค์กร

### สรุปเหตุการณ์ด้านความปลอดภัย โดยแสดงสถานะ ระดับความรุนแรง ผลกระทบ และ Top 10 Incidents

|  |  |  |
| --- | --- | --- |
| **ประเภทของภัยคุกคาม** | **ระดับความรุนแรง** | **จำนวนเหตุการณ์** |
|
| **Server Compromise** | | **1** |
| Brute Force Login Attack Failed | Medium (P3) | 1 |
| **Suspicious Activity** | | **5** |
| Inbound Communication With Blacklist IP Address | Medium (P3) | 5 |
| **รวม** | | **6** |

สรุปแนวโน้มการโจมตี

****

แสดงสถิติเหตุการณ์การโจมตีในแต่ละเดือน

### สรุปจำนวนอุปกรณ์ที่ส่ง Log

| **No.** | **Device Name** | **Device Type** | **IP Address** | **Remark** |
| --- | --- | --- | --- | --- |
| 1 | SFVUNL | Firewall | 203.150.51.61 | nan |
| 2 | SAMApplication | Windows Server | 203.150.51.53 | nan |
| 3 | SAMSQL | Windows Server | 203.150.51.52 | nan |
| 4 | SAMFILE | Windows Server | 203.150.51.51 | nan |
| 5 | SAMDC1 | Windows Server | 203.150.51.50 | nan |
| 6 | SAMBONANZA | Windows Server | 203.150.51.49 | nan |
| 7 | innotech\_01-PRD | Linux Server | 203.150.51.55 | nan |

### สรุปค่าเฉลี่ยจำนวน Log

|  |  |
| --- | --- |
| **ชื่อหน่วยงาน** | **หน่วย GB/Day** |
| บริษัท หลักทรัพย์จัดการกองทุน เอ็กซ์สปริง จำกัด | 1.9768 |

### ภาคผนวก

| **No.** | **Category** | **Name** | **Description** | **Priority** |
| --- | --- | --- | --- | --- |
| 1 | Suspicious Activity | DDoS Outbound Flood Traffic | เกิดเหตุการณ์มีการเชื่อมต่อจากภายในหน่วยงานหลายเครื่องออกไปสู่ภายนอก เกิดจำนวน/ครั้ง ภายในช่วงเวลาที่กำหนด | Critical (P1) |
| 2 | Suspicious Activity | Denial of Service Attack - External | เกิดเหตุการณ์การแจ้งเตือนเมื่อพบการโจมตีโดยมีจุดมุ่งหมายทำให้ระบบไม่สามารถให้บริการได้ โดยมี Traffic เกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด | Critical (P1) |
| 3 | Suspicious Activity | Denial of Service Attack - Internal | เกิดเหตุการณ์การแจ้งเตือนเมื่อพบการโจมตีโดยมีจุดมุ่งหมายทำให้ระบบไม่สามารถให้บริการได้ โดยมี Traffic เกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด | Critical (P1) |
| 4 | Suspicious Activity | Distributed Denial of Service Attack | เกิดเหตุการณ์การแจ้งเตือนเมื่อพบการโจมตีโดยมีจุดมุ่งหมายทำให้ระบบไม่สามารถให้บริการได้ โดยมี Traffic เกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด | Critical (P1) |
| 5 | Suspicious Activity | DoS Outbound Flood Traffic | เกิดเหตุการณ์มีการเชื่อมต่อจากภายในหน่วยงานออกไปสู่ภายนอกจำนวนหลายเครื่อง เกิดจำนวน/ครั้ง ภายในช่วงเวลาที่กำหนด | Critical (P1) |
| 6 | Suspicious Activity | Outbound-Communication With Blacklist IP Address Pass | เกิดเหตุการณ์การเชื่อมต่อจากอุปกรณ์ภายในออกไปยังจากอุปกรณ์ภายนอกที่มี IP Blacklist โดย Firewall ทำการปล่อยผ่าน Traffic | Critical (P1) |
| 7 | Malware | Mimikatz Detect | ตรวจพบโปรแกรมที่เป็นอันตรายชื่อ Mimikatz จาก Log อุปกรณ์ | High (P2) |
| 8 | Malware | Virus or Spyware Detected but Failed to Clean | เกิดเหตุการณ์แจ้งเตือน เมื่อตรวจพบ Log จาก Anti-Virus หรือ Anti-Spyware ว่ามีการแพร่กระจาย Malware ชนิดเดียวกัน จาก file เดียวกัน ภายในเครื่องเดียวกัน เกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด | High (P2) |
| 9 | Server Compromise | Brute Force Login Attack Success | เกิดเหตุการณ์ที่กรอกรหัสผ่านสำเร็จ ภายในจำนวนครั้งที่กำหนด | High (P2) |
| 10 | Suspicious Activity | Outbound-Communication With Blacklist IP Address Block | เกิดเหตุการณ์การเชื่อมต่อจากอุปกรณ์ภายในออกไปยังจากอุปกรณ์ภายนอกที่มี IP Blacklist โดย Firewall ทำการ BlockTraffic | High (P2) |
| 11 | Suspicious Activity | Outbound-Communication With Suspicious URL | ตรวจพบเหตุการณ์การเชื่อมต่อของอุปกรณ์กับ URL ที่เป็นอันตราย | High (P2) |
| 12 | Suspicious Activity | Outbound Flood Traffic | เกิดเหตุการณ์มีการเชื่อมต่อจากภายในหน่วยงานออกไปสู่ภายนอกเกิดจำนวน/ครั้ง ภายในช่วงเวลาที่กำหนด | High (P2) |
| 13 | Suspicious Activity | RDP Access from Suspicious IP | ตรวจสอบพบเหตุการณ์ มีการเชื่อมต่อจากภายนอก Blacklist IP เข้ามาที่เครื่องภายในองค์กรด้วย Port RDP 3389 | High (P2) |
| 14 | Suspicious Activity | SSH Access from Suspicious IP | ตรวจสอบพบเหตุการณ์ มีการเชื่อมต่อจากภายนอก Blacklist IP เข้ามาที่เครื่องภายในองค์กรด้วย Port SSH 22 | High (P2) |
| 15 | System Error | Monitored Log Source Stopped Sending Events | เกิดเหตุการณ์แจ้งเตือนเมื่อตรวจพบว่าอุปกรณ์หยุดการส่ง Log มายังระบบเกินกว่า ระยะเวลาที่กำหนด | High (P2) |
| 16 | Web Compromise | Cross-Site Scripting (Custom Detected) | เกิดเหตุการณ์บุกรุกเว็บไซต์ด้วยวิธีการ Cross site script โดยตรวจจับผ่าน Log web access | High (P2) |
| 17 | Web Compromise | Cross-Site Scripting (System Detected) Pass | เกิดเหตุการณ์บุกรุกเว็บไซต์ด้วยวิธีการ Cross site script โดยตรวจจับผ่าน WAF | High (P2) |
| 18 | Web Compromise | Directory Traversal (Custom) | เกิดเหตุการณ์บุกรุกเว็บไซต์ด้วยวิธีการ Directory Traversal โดยตรวจจับผ่าน Log web access | High (P2) |
| 19 | Web Compromise | Directory Traversal (System Detected) | เกิดเหตุการณ์บุกรุกเว็บไซต์ด้วยวิธีการ Directory Traversal โดยตรวจจับผ่าน WAF | High (P2) |
| 20 | Web Compromise | SQL Injection (Custom Detected) | เกิดเหตุการณ์บุกรุกเว็บไซต์ด้วยวิธีการ SQL Injection ตรวจจับผ่าน Log web access | High (P2) |
| 21 | Web Compromise | SQL Injection (System Detect) Pass | เกิดเหตุการณ์บุกรุกเว็บไซต์ด้วยวิธีการ SQL Injection โดยตรวจจับผ่าน WAF | High (P2) |
| 22 | Malware | Virus or Spyware Detected | เกิดเหตุการณ์การแจ้งเตือนจากโปรแกรม Anti-Virus หรือ Anti-Spyware ว่ามีการแพร่กระจาย Malware ภายในเครือข่าย | Medium (P3) |
| 23 | Server Compromise | Brute Force Login Attack Failed | เกิดเหตุการณ์ที่กรอกรหัสผ่านไม่สำเร็จเกินจำนวน/ครั้ง ภายในช่วงเวลาที่กำหนด | Medium (P3) |
| 24 | Suspicious Activity | Host Sending Excessive Email | เกิดเหตุการณ์แจ้งเตือนเมื่อตรวจพบ Host ที่ไม่ได้กำหนดให้เป็น Mail Server พยายามส่ง E-mail ไปยัง Host เดียว หรือ หลาย Host มากผิดปกติ | Medium (P3) |
| 25 | Suspicious Activity | Inbound Communication With Blacklist IP Address | เกิดเหตุการณ์การเชื่อมต่อมาจากอุปกรณ์ที่มี IP Blacklist ภายนอกองค์กรมายังอุปกรณ์ภายในองค์กร | Medium (P3) |
| 26 | Web Compromise | Cross-Site Scripting (System Detected) Block | เกิดเหตุการณ์บุกรุกเว็บไซต์ด้วยวิธีการ Cross site script โดยตรวจจับผ่าน WAF | Medium (P3) |
| 27 | Web Compromise | Directory Traversal (System Detected) | เกิดเหตุการณ์บุกรุกเว็บไซต์ด้วยวิธีการ Directory Traversal โดยตรวจจับผ่าน WAF | Medium (P3) |
| 28 | Web Compromise | SQL Injection (System Detect) Block | เกิดเหตุการณ์บุกรุกเว็บไซต์ด้วยวิธีการ SQL Injection โดยตรวจจับผ่าน WAF | Medium (P3) |
| 29 | Web Compromise | Suspicious Post from Untrusted Source | เกิดเหตุการณ์แจ้งเตือนเมื่อตรวจพบการเข้าถึง URL ที่มีความผิดปกติ | Medium (P3) |
| 30 | Information Gathering | High Threat Targeting Vulnerable Asset | เกิดเหตุการณ์พยายามโจมตีเข้าสู่ระบบที่มีความเสี่ยงสูง หรือมีช่องโหว่อยู่ | Low (P4) |
| 31 | Information Gathering | Port Scan | เกิดเหตุการณ์แจ้งเตือนเมื่อตรวจพบการพยายาม Scan Port ต่าง ๆ หลาย Port ไปยังเครื่องเป้าหมายเครื่องเดียว เกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด | Low (P4) |
| 32 | Information Gathering | Port Sweep | เกิดเหตุการณ์แจ้งเตือนเมื่อตรวจพบ การพยายาม Scan เครือข่าย โดยการเจาะจง Port ไปยังเครื่องต่าง ๆ เกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด | Low (P4) |
| 33 | Information Gathering | Vulnerability Scanner Detected (by events) | เกิดเหตุการณ์แจ้งเตือนเมื่อตรวจพบการ Scan ค้นหาช่องโหว่ของระบบ | Low (P4) |
| 34 | Suspicious Activity | Delegate Authentication Request | ตรวจพบ Event Delegate Authentication Request | Critical (P1) |
| 35 | Suspicious Activity | Delegate Access | ตรวจพบ Event Delegate Access | Critical (P1) |