**รายงานสรุปผลการปฏิบัติงาน  
 ศูนย์เฝ้าระวังความปลอดภัยระบบคอมพิวเตอร์ และสารสนเทศ**

**(Security Operation Center)**

**ประจำเดือน {{month}} {{year}}**

**{{name\_capany}}**

**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** **{{month}} {{year}}**

**เสนอ**

**{{name\_capany}}**

**จัดทำโดย {{** **Service\_provider}}**

## 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 และสารสนเทศที่เกิดขึ้นในเดือน{{month}} {{year}} โดยมีรายละเอียดดังนี้

### ภาพรวมของการเฝ้าระวังเหตุการณ์ด้านความปลอดภัย (Security Incident)

จากผลการเฝ้าระวังประจำเดือน {{month}} {{year}} ตรวจพบเหตุการณ์ที่สำคัญ ดังรายละเอียด ต่อไปนี้

| **ลำดับ** | **ชื่อหน่วยงาน** | **จำนวนเหตุการณ์** | **CRITICAL** | **HIGH** | **MEDIUM** | **LOW** |
| --- | --- | --- | --- | --- | --- | --- |
| 1. | {{name\_capany}} | {{sum}} | {{crit}} | {{high}} | {{medium}} | {{low}} |

มีเหตุการณ์ที่น่าสนใจดังนี้{% if sum > 0%}{% for data in all\_event %}

1. {{data.vul}}

|  |  |  |
| --- | --- | --- |
| **{%tc for col in data.col\_label %}** | **{{ col }}** | **{%tc endfor %}** |
| {%tr for item in data. cols %} | | |
| {%tc for col in item.event %} | {{ col }} | {%tc endfor %} |
| {%tr endfor %} | | |

**คำแนะนำ**

{{data.detail}}

{%endfor %}{% else %}

* ไม่พบการโจมตีใดๆ ในช่วงเวลาดังกล่าว{% endif %}

### สรุปเหตุการณ์ด้านความปลอดภัย โดยแสดงสถานะ ระดับความรุนแรง ผลกระทบ และ Top 10 Incidents{% if sum > 0%}

|  |  |  |
| --- | --- | --- |
| **ประเภทของภัยคุกคาม** | **ระดับความรุนแรง** | **จำนวนเหตุการณ์** |
|
| {%tr for data in category %} | | |
| **{{data.category}}** | | **{{data.count}}** |
| {%tr for item in data.event %} | | |
| {{item.type}} | {{item.priority}} | {{item.count}} |
| {%tr endfor %} | | |
| {%tr endfor %} | | |
| **รวม** | | **{{category\_count}}** |

{% else %}

* ไม่พบการโจมตีใดๆ ในช่วงเวลาดังกล่าว{% endif %}

สรุปแนวโน้มการโจมตี

**{{graph}}**

แสดงสถิติเหตุการณ์การโจมตีในแต่ละเดือน

### สรุปจำนวนอุปกรณ์ที่ส่ง Log

| **No.** | **Device Name** | **Device Type** | **IP Address** | **Remark** |
| --- | --- | --- | --- | --- |
| {%tr for data in device%} | | | | |
| {{data.no}} | {{data.name}} | {{data.type}} | {{data.address}} |  |
| {%tr endfor %} | | | | |

### สรุปค่าเฉลี่ยจำนวน Log

|  |  |
| --- | --- |
| **ชื่อหน่วยงาน** | **หน่วย GB/Day** |
| {{name\_capany}} | {{capa}} |

### ภาคผนวก

| **No.** | **Category** | **Name** | **Description** | **Priority** |
| --- | --- | --- | --- | --- |
| {%tr for data in vulnerability%} | | | | |
| {{data.no}} | {{data.category}} | {{data.name\_en}} | {{data.detail\_th}} | {{data.priority}} |
| {%tr endfor %} | | | | |