ขอบเขตของงาน (Terms of Reference : TOR)
จ้างเหมาบริการศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (SOC) บริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (SIEM) และระบบการสังเกตการณ์แบบรวมศูนย์

1. ความเป็นมา

สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) (สขญ.) มีภารกิจในการบริหารจัดการและให้บริการข้อมูลขนาดใหญ่ เพื่อสนับสนุนการดำเนินงานของภาครัฐ การกำหนดนโยบาย และการพัฒนาประเทศ โดยมีการใช้งานระบบสารสนเทศและโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่มีความสำคัญ ครอบคลุมทั้งระบบภายใน On-premises และระบบ Cloud Computing ได้แก่ Amazon Web Services (AWS), Microsoft Azure และ Google Cloud Platform (GCP), Huawei Cloud, GDCC Cloud และ GDCC OpenData รวมถึงสภาพแวดล้อมแบบ Container และ Kubernetes

จากสภาพแวดล้อมทางเทคโนโลยีที่มีความหลากหลายและซับซ้อนดังกล่าว ทำให้ สขญ. ต้องเผชิญกับภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ที่มีแนวโน้มเพิ่มขึ้น ทั้งในรูปแบบของการโจมตีระบบเครือข่าย การบุกรุกระบบ การใช้สิทธิ์โดยมิชอบ และการโจมตีระบบ Cloud ซึ่งอาจส่งผลกระทบต่อความต่อเนื่องในการให้บริการ ความน่าเชื่อถือของข้อมูล และภารกิจสำคัญของภาครัฐ

ปัจจุบัน สขญ. มีความจำเป็นต้องยกระดับการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างทันท่วงที และสอดคล้องกับแนวปฏิบัติสากล สขญ. จึงมีความจำเป็นต้องจัดหาและจ้างบริการศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (SOC) ที่พร้อมสนับสนุนระบบที่เกี่ยวข้อง ได้แก่ ระบบ SIEM ระบบการสังเกตการณ์และตรวจจับเหตุการณ์ขั้นสูง ระบบแจ้งเตือน และระบบแสดงผลภาพรวมสถานการณ์แบบรวมศูนย์ เพื่อรองรับการดำเนินพันธกิจของ สขญ. อย่างมั่นคงและต่อเนื่อง

2. วัตถุประสงค์

2.1 เพื่อจัดหาบริการศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (SOC) สำหรับเฝ้าระวัง ตรวจจับ และตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ของทาง สขญ.

2.2 เพื่อให้ สขญ. มีระบบรวบรวม วิเคราะห์ และบริหารจัดการข้อมูลบันทึกเหตุการณ์ (Log) จากระบบสารสนเทศทั้งแบบ On-premises Cloud และ Container อย่างเป็นระบบและตรวจสอบได้

2.3 เพื่อเพิ่มประสิทธิภาพในการตรวจจับ วิเคราะห์ และแจ้งเตือนภัยคุกคามทางไซเบอร์ ด้วยระบบ SIEM และเทคโนโลยีสนับสนุนที่มีคุณสมบัติเทียบเท่ามาตรฐานสากล โดยไม่จำกัดยี่ห้อหรือผู้ผลิต

2.4 เพื่อรองรับการจัดเก็บข้อมูลบันทึกเหตุการณ์ในระบบของ สขญ. เพื่อใช้ในการตรวจสอบย้อนหลังและจัดทำรายงาน

2.5 เพื่อจัดให้มีระบบแจ้งเตือนและกระบวนการตอบสนองต่อเหตุการณ์ที่มีขอบเขตและระยะเวลาการตอบสนองที่ชัดเจน และสามารถเชื่อมต่อกับระบบบริหารจัดการเหตุการณ์เดิมของทาง สขญ. ได้

3. คุณสมบัติของผู้เสนอราคา

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการ ผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพตามที่ประกาศ

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่น หรือกระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกันซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องครบถ้วนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e-GP) ของกรมบัญชีกลาง

3.11 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

1. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหรือต่างประเทศ ซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ งบแสดงฐานะการเงิน 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ หมายถึง งบแสดงฐานะการเงินย้อนไปก่อนวันที่หน่วยงานของรัฐกำหนดให้เป็นวันยื่นข้อเสนอ 1 ปีปฏิทิน เว้นแต่กรณีนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หากวันยื่นข้อเสนอเป็นช่วงระยะเวลาที่กรมพัฒนาธุรกิจการค้ากำหนดให้นิติบุคคลยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ซึ่งจะอยู่ในช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปี โดยนิติบุคคลที่เป็นผู้ยื่นข้อเสนอนั้นยังอยู่ในช่วงของการยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า คือ ช่วงเดือนมกราคม - เดือนพฤษภาคม กรณีนี้ให้สามารถยื่นงบแสดงฐานะการเงินย้อนไปอีก 1 ปี ได้

2. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า หรือกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงิน ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า 1 ล้านบาท

3. สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน 500,000 บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา ให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน 90 วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอ ในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

4. กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ สามารถดำเนินการได้ดังนี้

(1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หรือบุคคลธรรมดาที่ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง

(2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดาที่มิได้ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคาร แห่งประเทศไทยแจ้งเวียนให้ทราบ หรือเป็นสินเชื่อที่ธนาคารต่างประเทศหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารกลางต่างประเทศนั้น ตามรายชื่อบริษัทที่ธนาคารกลางต่างประเทศนั้นแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน

5. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดาที่มิได้ถือสัญชาติไทยตามข้อ 2 ข้อ 3 และข้อ 4 (2) มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตราตามประกาศที่ธนาคารแห่งประเทศไทยกำหนด ในช่วงระหว่างวันที่เผยแพร่ประกาศและเอกสารประกวดราคาในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e - GP) จนถึงวันเสนอราคา

ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องยื่นเอกสารที่แสดงให้เห็นถึงข้อมูลเกี่ยวกับมูลค่าสุทธิของกิจการแล้วแต่กรณีประกอบกับเอกสารดังกล่าวจะต้องผ่านการรับรองตามระเบียบกระทรวงการต่างประเทศว่าด้วยการรับรองเอกสาร พ.ศ. 2539 และที่แก้ไขเพิ่มเติมกำหนด โดยจะต้องยื่นเอกสารดังกล่าวในวันยื่นข้อเสนอ หากผู้ยื่นข้อเสนอมิได้มีการยื่นเอกสารดังกล่าวมาพร้อมกับการยื่นข้อเสนอให้ถือว่าผู้ยื่นข้อเสนอรายนั้นยื่นเอกสารไม่ครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา

6. กรณีตาม ข้อ 1 - ข้อ 5 ไม่ใช้บังคับกรณีดังต่อไปนี้

(6.1) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐภายในประเทศ

(6.2) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย พ.ศ. 2483 และที่แก้ไขเพิ่มเติม

(6.3) งานจ้างก่อสร้างที่กรมบัญชีกลางได้ขึ้นทะเบียนผู้ประกอบการงานก่อสร้างแล้ว และงานจ้างก่อสร้างที่หน่วยงานของรัฐที่ได้มีการจัดทำบัญชีผู้ประกอบการงานก่อสร้างที่มีคุณสมบัติเบื้องต้นไว้แล้วก่อนวันที่พระราชบัญญัติการจัดซื้อจัดจ้างฯ มีผลใช้บังคับ

(6.4) การจัดซื้อจัดจ้างตามมาตรา 56 วรรคหนึ่ง (2) (ข) และ (ค) แห่งพระราชบัญญัติการจัดซื้อจัดจ้างฯ

(6.5) การซื้ออสังหาริมทรัพย์และการเช่าอสังหาริมทรัพย์

(6.6) กรณีงานจ้างบริการหรืองานจ้างเหมาบริการกับบุคคลธรรมดา เช่น จ้างพนักงานขับรถ ครูชาวต่างชาติ พนักงานเก็บขยะ พนักงานบันทึกข้อมูล เป็นต้น

3.12 ผู้ยื่นข้อเสนอจะต้องมีผลงานการจ้างเหมาบริการศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (SOC) บริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (SIEM) และระบบการสังเกตการณ์แบบรวมศูนย์ หรือบริการเฝ้าระวังความมั่นคงปลอดภัยระบบสารสนเทศ หรืองานในลักษณะเดียวกัน ให้หน่วยงานภาครัฐ หรือเอกชนที่น่าเชื่อถือได้ มูลค่าโครงการไม่ต่ำกว่า 1,000,000 บาท (หนึ่งล้านบาทถ้วน) ต่อสัญญา และเป็นผลงานที่ดำเนินการแล้วเสร็จ หรือเป็นโครงการที่อยู่ระหว่างการให้บริการ โดยเป็นผลงานย้อนหลังไม่เกิน 5 ปี นับถึงวันยื่นข้อเสนอ โดยแสดงหลักฐานเป็นสำเนาสัญญา หรือใบสั่งซื้อหรือสั่งจ้าง หรือหนังสือรับรองผลงาน อย่างน้อย 1 ผลงาน

4. ขอบเขตของงาน

4.1 **ผู้ให้บริการต้องปฏิบัติตามข้อกำหนดเงื่อนไขเทคโนโลยีและแพลตฟอร์ม** สำหรับจัดทำระบบบริหารจัดการเหตุและสังเกตการณ์ (SIEM & Observation platform) โดยมีคุณสมบัติอย่างน้อยดังต่อไปนี้

4.1.1 ข้อกำหนดพื้นฐานของระบบที่ผู้ให้บริการมีความประสงค์ที่จะนำมาใช้กับทาง สขญ. จะต้องมีคุณสมบัติอย่างน้อยดังต่อไปนี้

4.1.1.1 รองรับการทำงานบนสภาพแวดล้อมแบบ Multi-Cloud และ On-premise ซึ่งให้บริการเช่น Network Device, Firewall, IDS/IPS, บนผู้ให้บริการ Cloud platform เช่น AWS, Azure, GCP, Huawei Cloud, , GDCC Cloud, GDCC OpenData, ระบบ Container / Kubernetes, ระบบ Windows และ Linux และระบบอื่นๆตามที่ สขญ. ระบุในเอกสารแนบ เป็นอย่างน้อย

4.1.2 **ข้อกำหนด ระบบบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (SIEM) ที่ผู้ให้บริการมีความประสงค์ที่จะนำมาใช้กับทาง สขญ. จะต้องมีคุณสมบัติอย่างน้อยดังต่อไปนี้**

4.1.2.1 ระบบการบริหารจัดการปริมาณข้อมูล (Log Volume Management) ต้องมีความยืดหยุ่นในการบริหารจัดการข้อมูลเพื่อประสิทธิภาพสูงสุด และป้องกันข้อมูลสูญหายในช่วงที่มีปริมาณข้อมูลพุ่งสูง (Burst volume) โดยผู้ให้บริการต้องนำเสนอรูปแบบการบริหารจัดการข้อมูล รูปแบบใดรูปแบบหนึ่ง ดังต่อไปนี้

1. **รูปแบบที่ 1**: การคิดตามจำนวนอุปกรณ์ (Endpoint-Based) ไม่น้อยกว่า 1,000 Endpoint ต่อเดือน

- ระบบต้องรองรับปริมาณข้อมูล Log แบบไม่จำกัดปริมาณ และไม่จำกัดความเร็วในการรับข้อมูล (Unlimited event per second)
- เนื่องจากเป็นรูปแบบไม่จำกัดปริมาณข้อมูล จึงได้รับการยกเว้นเงื่อนไขการถัวเฉลี่ยรายเดือนและข้อมูลสำรอง **โดยระบบต้องประมวลผลข้อมูลที่เข้ามาได้ทั้งหมดไม่ว่าจะมีปริมาณพุ่งสูง เพียงใดก็ตาม**
- ในกรณีของสภาพแวดล้อมระบบคอนเทนเนอร์ (Container) การนับจำนวนอุปกรณ์ Endpoint หรือเทียบเท่า ให้คำนวณและนับจากจำนวนเครื่องแม่ข่ายหลักที่ใช้ประมวลผล (Worker Nodes หรือ Virtual Machine Instances) เท่านั้น โดยผู้ให้บริการจะต้อง**ไม่นำจำนวนหน่วยประมวลผลย่อย (Pods หรือ Containers) ภายในระบบมานับรวมเพื่อหักลบในโควตาการให้บริการอย่างเด็ดขาด**
- ระบบที่นำเสนอจะต้องรองรับการอ่านและแยกแยะ ข้อมูลเชิงลึก (Metadata) ของระบบคอนเทนเนอร์ (Container) เช่น Pod Name, Namespace, Container ID ที่ถูกแนบมาในเนื้อหาของข้อมูลจราจรคอมพิวเตอร์ (Log Payload) ในรูปแบบ JSON หรือรูปแบบมาตรฐานอื่น ๆ ได้ เพื่อสนับสนุนให้ศูนย์ปฏิบัติการ SOC สามารถวิเคราะห์และระบุต้นตอของภัยคุกคามในระดับแอปพลิเคชันย่อยได้อย่างแม่นยำ โดยต้องไม่นำข้อมูลส่วนนี้ไปคิดเป็นจำนวนโควตา (Endpoint) เพิ่มเติม

2. **รูปแบบที่ 2**: การคิดตามปริมาณข้อมูลรวมไม่น้อยกว่า 60 GB ต่อวัน
   - การบริหารโควตาแบบเฉลี่ยรายเดือน: ปริมาณข้อมูลที่เกินโควตา 60 GB ในบางวัน จะ**ต้องสามารถนำไปถัวเฉลี่ย**กับวันที่มีการใช้งานน้อยภายในเดือนเดียวกันได้ โดยระบบต้องทำการประมวลผลข้อมูลได้ทั้งหมดตราบใดที่ยอดรวมรายเดือนยังไม่เกินโควตา (เช่น เดือนที่มี 30 วัน = 1,800 GB/เดือน)
   - ปริมาณข้อมูลสำรองฉุกเฉินรายปี (Volume Buffer): ผู้ให้บริการต้องจัดสรรปริมาณข้อมูลสำรองให้อย่างน้อย 4.28 TB ต่อปี โดยไม่คิดค่าใช้จ่ายเพิ่มเติม เพื่อใช้หักลบในกรณีที่ปริมาณการใช้งานแบบเฉลี่ยรายเดือน มีการใช้งานเกินกว่าโควตารายเดือนที่กำหนด
   - การจัดการข้อมูลเมื่อเกินโควตาทั้งหมด: ในกรณีที่ สขญ. ใช้งานเกินโควตารายเดือน และปริมาณข้อมูลสำรองฉุกเฉิน (Volume Buffer) ถูกใช้จนหมดแล้ว ระบบจะต้องยังคงสามารถรับข้อมูล เข้ามาจัดเก็บได้โดย **ข้อมูลต้องไม่สูญหายอย่างเด็ดขาด** ทั้งนี้ ผู้ให้บริการอาจจำกัดเฉพาะสิทธิ์ การประมวลผล (Active Processing) ให้**อยู่ในเพดานโควตาเดิม** จนกว่าจะขึ้นรอบเดือนใหม่
   - รองรับการส่งข้อมูลจากระบบต่าง ๆ โดยไม่จำกัดจำนวนบริการ อุปกรณ์ และ IP Address

3. **ข้อกำหนดมาตรฐาน** ที่ผู้ให้บริการต้องมีไม่ว่าจะเป็นรูปแบบใดรูปแบบหนึ่งก็ตาม มีดังนี้
   - ทาง สขญ. **ต้องสามารถค้นหาและจัดเก็บ Log ย้อนหลังอย่างน้อย 90 วัน** เพื่อให้สอดคล้องตาม หลักเกณฑ์การเก็บรักษาข้อมูลจราจร และ พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ รวมถึงสอดคล้องกับแนวปฏิบัติมาตรฐานสากล เช่น ISO 27001 หรือ NIST
   - ผู้ให้บริการต้องจัดให้มีกลไกและเครื่องมือในการคัดกรอง แยกแยะ และปิดบังข้อมูล (Data Masking) / Anonymization) เพื่อคัดแยกข้อมูลตามชั้นความลับของข้อมูล (Data Classification) **ตามมาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (สพร.)** และกฎหมายอื่นที่เกี่ยวข้อง ก่อนที่จะมีการส่งข้อมูล Log ออกนอกประเทศไทย
   - ผู้ให้บริการต้องมีระบบกรองข้อมูล Log (Log Filtering) ตั้งแต่ระบบต้นทาง (Source Agent) **เพื่อเลือกส่งเฉพาะข้อมูล Log ที่จำเป็นต่อการวิเคราะห์และเฝ้าระวังภัยคุกคามทางไซเบอร์เท่านั้น** เพื่อลดการใช้ช่องสัญญาณ (Bandwidth) และพื้นที่จัดเก็บโดยไม่จำเป็น และมีระบบบริหารจัดการเนื้อที่จัดเก็บข้อมูล (Log Rotation) ที่มีประสิทธิภาพ โดยไม่ทำให้ระบบหลักหยุดชะงัก
   - **ข้อมูล Log ทั้งหมดที่ส่งออกจะต้องได้รับการเข้ารหัสข้อมูลระหว่างการรับส่ง** (Data in Transit Encryption) ด้วยโปรโตคอลความปลอดภัยระดับสากล เช่น TLS 1.3 หรือเทียบเท่า และมีการเข้ารหัสขณะจัดเก็บ (Data at Rest Encryption) บนระบบ Cloud ปลายทาง
   - ศูนย์จัดเก็บข้อมูล (Data Center) หรือบริการ Cloud ในต่างประเทศของผู้ให้บริการ จะต้องได้รับมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศอย่างใดอย่างหนึ่งเป็นอย่างน้อย ได้แก่ ISO/IEC 27001, ISO/IEC 27017 (Cloud Security) หรือ SOC 2 Type II **โดยต้องแสดงเอกสารรับรอง ที่ยังไม่หมดอายุ ณ วันยื่นข้อเสนอ**
   - ระบบที่นำเสนอจะต้องรองรับการนำเข้าข้อมูล (Ingestion) ของ Native log data จาก Third-party security tools และต้องรองรับ Generic log format อย่างน้อย CEF, LEEF, Syslog, JSON / HTTP JSON และมีเครื่องมือ Custom parser / Generic log parser **สำหรับแหล่งข้อมูลที่ไม่มี Parser สำเร็จรูป**

4.1.2.2 กฎเกณฑ์การตรวจจับ (Detection Rules): มีชุดกฎเกณฑ์มาตรฐาน (Out-of-the-box Rules) ที่ครอบคลุมรูปแบบการโจมตีสากล (Predefined Rules) และรองรับให้ สขญ. สามารถสร้างหรือปรับแต่งกฎเพิ่มเติม (Custom Rules) ได้เอง

4.1.2.3 การวิเคราะห์และประเมินความเสี่ยงเชิงลึก

1. มีระบบการวิเคราะห์พฤติกรรมผู้ใช้และทรัพย์สิน (UEBA) เพื่อวิเคราะห์ความผิดปกติ แสดงระดับความเสี่ยง และแสดงกราฟความสัมพันธ์ของการโจมตี

2. มีระบบจัดลำดับความสำคัญและความรุนแรงของช่องโหว่และเหตุการณ์ (Risk Prioritization) โดยอ้างอิงตามมาตรฐานสากล เช่น CVSS, MITRE ATT&CK Framework

4.1.2.4 การเชื่อมต่อและการแสดงผลภาพรวม (Integration & Dashboard)

1. มีหน้าจอแสดงผลแบบรวมศูนย์ (Centralized Dashboard) โดยต้องเปิดสิทธิ์ให้บุคลากรของ สขญ. เข้าถึงเพื่อดูข้อมูล สืบสวนเชิงลึกด้วยตนเอง และออกรายงานตามมาตรฐานสากลได้
2. รองรับการเชื่อมต่อกับระบบป้องกันภัยอื่นๆ เช่น EDR, NDR และอุปกรณ์เครือข่ายของ สขญ. ผ่านช่องทางมาตรฐาน ได้แก่ API, Webhook, Syslog หรือ Native Connector โดยต้องทำงานร่วมกันได้และไม่มีการคิดค่าใช้จ่ายในการพัฒนาเพิ่มเติม

4.1.2.5 ระบบแจ้งเตือน (Alert & Notification): รองรับการแจ้งเตือนความผิดปกติแบบ Real-time หรือ Near Real-time ผ่านช่องทางมาตรฐาน ได้แก่ อีเมล และ MS Teams เป็นอย่างน้อย รวมถึงรองรับการขยายช่องทางผ่าน API หรือ Webhook

4.1.3 **ข้อกำหนด ระบบข้อมูลภัยคุกคามเชิงลึก (Threat Intelligence) ที่ผู้ให้บริการมีความประสงค์ที่จะนำมาใช้กับทาง สขญ. จะต้องมีคุณสมบัติอย่างน้อยดังต่อไปนี้**

4.1.3.1 ด้านแหล่งข้อมูลภัยคุกคาม (Threat Intelligence Feed): ระบบต้องรองรับการเชื่อมต่อและดึงข้อมูลภัยคุกคามจากแหล่งข้อมูลเปิด (OSINT) เป็นอย่างน้อย โดยต้องรองรับการเชื่อมต่อตามรูปแบบมาตรฐานสากล เช่น STIX/TAXII เพื่อให้สามารถทำงานร่วมกับแหล่งข้อมูลที่หลากหลายได้

4.1.3.2 ต้องสามารถเชื่อมโยงตรวจสอบความสัมพันธ์ (Correlate) ระหว่าง Log ภายใน สขญ. กับ Threat Intelligence ได้อัตโนมัติ

4.1.4 **ข้อกำหนด ระบบตรวจจับและตอบสนองภัยคุกคามบนอุปกรณ์ปลายทาง (Host หรือ Agent) ที่ผู้ให้บริการมีความประสงค์ที่จะนำมาใช้กับทาง สขญ. จะต้องมีคุณสมบัติอย่างน้อยดังต่อไปนี้**

4.1.4.1 ต้องรองรับการทำงานบนระบบปฏิบัติการที่หลากหลาย ได้แก่ Windows, Linux และ macOS ในเวอร์ชันที่องค์กรใช้งานอยู่หรือตามที่องค์กรร้องขอ

4.1.4.2 สามารถตรวจจับและอ้างอิงพฤติกรรมของภัยคุกคามตามกรอบมาตรฐาน เช่น MITRE ATT&CK Framework ได้ และสามารถบอก Techniques, Tactics ของการโจมตีที่เกิดขึ้นโดยอ้างอิงตาม MITRE ATT&CK ได้ และสามารถ Link ออกไปยัง MITRE Website เพื่ออ่านรายละเอียดเทคนิคได้

4.1.4.3 ระบบที่ผู้ให้บริการนำเสนอจะต้องสามารถเชื่อมต่อและบูรณาการข้อมูล (Integration) ร่วมกับระบบรักษาความปลอดภัยทางอีเมล (Email Security) ที่ สขญ. ใช้งานอยู่ในปัจจุบัน ได้แก่ Microsoft Defender for Office 365 เพื่อวิเคราะห์และเชื่อมโยงเหตุการณ์ภัยคุกคามที่เกิดขึ้นต่อเนื่องกันได้

4.1.5 **ข้อกำหนด ระบบตรวจจับและตอบสนองภัยคุกคามระดับเครือข่าย (Network Detection and Response) ที่ผู้ให้บริการมีความประสงค์ที่จะนำมาใช้กับทาง สขญ. จะต้องมีคุณสมบัติอย่างน้อยดังต่อไปนี้**

4.1.5.1 สามารถวิเคราะห์การจราจรบนเครือข่ายแบบเรียลไทม์ หรือ ใกล้เรียลไทม์

4.1.5.2 สามารถจัดเก็บและวิเคราะห์ Metadata ของโปรโตคอลเครือข่าย (เช่น HTTP, DNS, SMB)

4.1.5.3 สามารถบันทึกข้อมูลแบบ Full Packet Capture (PCAP) จาก Sensor ที่ติดตั้งในระบบเครือข่ายของ สขญ. สำหรับเหตุการณ์ที่ตรวจพบจาก IDS signature match และสามารถคัดลอกไฟล์ PCAP ดังกล่าวไปยังระบบภายนอกเพื่อใช้ในการสืบสวนเชิงลึกหรือวิเคราะห์เพิ่มเติมด้วยเครื่องมือภายนอก เช่น Wireshark ได้

4.1.5.4 ระบบต้องสามารถเชื่อมโยงข้อมูล (Correlation) ร่วมกับระบบตรวจจับและตอบสนองภัยคุกคามบนอุปกรณ์ปลายทาง เพื่อระบุต้นตอของภัยคุกคาม (Root Cause Analysis) ที่มีการเคลื่อนไหวผ่านเครือข่ายและอุปกรณ์ปลายทางได้

4.1.5.5 ระบบต้องสามารถเชื่อมโยง (Correlation) และจัดกลุ่มเหตุการณ์ที่เกี่ยวข้องกันโดยอัตโนมัติจากหลายแหล่งข้อมูล เช่น Network, Endpoint, Identity/User, Cloud และ Security Controls อื่น ๆ ให้อยู่ในรูปแบบ Case หรือ Incident เดียวกัน พร้อมแสดงความสัมพันธ์ของ Alert, Entity, Host, User, IP Address และลำดับการโจมตีตาม Kill Chain เพื่อช่วยระบุต้นตอของภัยคุกคาม (Root Cause Analysis) และสนับสนุนการสืบสวนเหตุการณ์ที่เคลื่อนไหวข้ามเครือข่ายและอุปกรณ์ปลายทางได้

4.1.6 **ข้อกำหนด ระบบการตอบสนองต่อภัยคุกคามอัตโนมัติ (SOAR) ที่ผู้ให้บริการมีความประสงค์ที่จะนำมาใช้กับทาง สขญ. จะต้องมีคุณสมบัติอย่างน้อยดังต่อไปนี้**

4.1.6.1 มีระบบการจัดการเหตุการณ์ บันทึกและติดตามสถานะของเหตุการณ์ (Incident Management) ตั้งแต่เริ่มต้นจนถึงการแก้ไขแล้วเสร็จ พร้อมบันทึกประวัติการดำเนินการทั้งหมด

4.1.6.2 การเชื่อมต่อและสั่งการแบบรวมศูนย์ (Integration & Orchestration): รองรับการเชื่อมต่อผ่านช่องทาง API หรือ Native Connector กับอุปกรณ์และระบบรักษาความปลอดภัยอื่น ๆ ของ สขญ. เช่น Firewall, Active Directory, EDR เพื่อสั่งการระงับเหตุการณ์จากศูนย์กลางได้ทันที เช่น การสั่ง Block IP Address หรือระงับสิทธิ์ผู้ใช้งาน

4.1.6.3 กระบวนการตอบสนอง (Playbooks): มีชุดคำสั่งการตอบสนองมาตรฐาน (Out-of-the-box Playbooks) เช่น การจัดการ Phishing Email หรือ Malware และเปิดให้ สขญ. สามารถสร้างหรือปรับแต่ง Playbook เพิ่มเติมได้เอง

4.1.6.4 ระบบต้องรองรับการตอบสนองอัตโนมัติอย่างเต็มรูปแบบสำหรับ Playbook ที่ได้รับการยืนยันและสรุปผลร่วมกันจาก สขญ. แล้ว ส่วนเหตุการณ์ที่ยังไม่มี Playbook รองรับ

ระบบต้องสามารถแจ้งเตือนเพื่อให้เจ้าหน้าที่ดำเนินการวิเคราะห์และแก้ไขแบบควบคุมเอง (Manual) ได้

4.1.6.5 การจัดการระดับความอัตโนมัติ (Automation & Manual Response):

1. แบบอัตโนมัติ (Fully Automated): ระบบต้องรองรับการตอบสนองอัตโนมัติอย่างเต็มรูปแบบ สำหรับ Playbook ที่ได้รับการยืนยันและอนุมัติจาก สขญ. แล้ว
2. แบบกึ่งอัตโนมัติ (Human-in-the-loop): รองรับการกำหนดเงื่อนไขให้ผู้ดูแลระบบเป็นผู้อนุมัติการทำงานก่อนระบบดำเนินการตอบสนอง เพื่อป้องกันผลกระทบต่อระบบปฏิบัติการหลัก
3. แบบควบคุมเอง (Manual): สำหรับเหตุการณ์ที่ยังไม่มี Playbook รองรับ ระบบต้องสามารถแจ้งเตือนเพื่อให้เจ้าหน้าที่ดำเนินการวิเคราะห์และแก้ไขปัญหาแบบควบคุมเองได้

4.2 **ผู้ให้บริการต้องจัดให้มีบริการศูนย์ปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (Managed SOC) เพื่อเฝ้าระวัง วิเคราะห์ ตรวจจับ และตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์** โดยใช้เทคโนโลยีและแพลตฟอร์มตามข้อ 4.1 โดยมีคุณสมบัติและขอบเขตการดำเนินงาน อย่างต่ำดังต่อไปนี้

4.2.1 รูปแบบการให้บริการและมาตรฐานการตรวจจับ

4.2.1.1 ให้บริการในรูปแบบ SOC อย่างเต็มรูปแบบ (Fully Managed SOC) โดยมีหน้าที่เฝ้าระวัง วิเคราะห์เชิงลึก คัดกรอง และตรวจจับเหตุการณ์ภัยคุกคามจากข้อมูล Log ตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์ (24x7) เพื่อลดภาระการคัดกรองการแจ้งเตือน (False Positive) เบื้องต้นของเจ้าหน้าที่ สขญ.

4.2.1.2 มีความสามารถในการตรวจจับ ตามวิธีมาตรฐานสากล เช่น วิเคราะห์ด้วย MITRE ATT&CK Framework ครอบคลุมทุกกลยุทธ์ (Tactics) ใน Enterprise Matrix โดยต้องรองรับเทคนิคการโจมตีอย่างน้อยดังต่อไปนี้:

1. Unauthorized Access และ Lateral Movement
2. Malware และ Ransomware
3. การลักลอบนำข้อมูลออก (Data Exfiltration)
4. Denial-of-Service (DoS)
5. Web-based Attacks เช่น SQL Injection, Cross-site Scripting
6. ทั้งนี้ ระบบและกระบวนการตรวจจับจะต้องได้รับการอัปเดตให้รองรับภัยคุกคามรูปแบบใหม่ๆ อย่างสม่ำเสมอ

4.2.2 การปรับแต่งระบบอย่างต่อเนื่อง: ผู้ให้บริการจะต้องมีกระบวนการทบทวนและปรับแต่งกฎเกณฑ์การตรวจจับ (Correlation Rules) ร่วมกับ สขญ. อย่างต่อเนื่องตลอดระยะเวลาสัญญา เพื่อลดอัตราการแจ้งเตือนที่ผิดพลาด (False Positive) ให้อยู่ในระดับที่น้อยที่สุด และเพิ่มความแม่นยำให้สอดคล้องกับการเปลี่ยนแปลงของระบบ สขญ.

4.2.3 ความปลอดภัยของช่องทางการสื่อสาร: ต้องสามารถรับส่งข้อมูลกับศูนย์ SOC ของผู้ให้บริการผ่านช่องทางที่ปลอดภัย เช่น VPN, TLS Encryption หรือเทียบเท่า ได้

4.2.4 ข้อระดับความรุนแรงและระยะเวลาการตอบสนอง (SLA): ผู้ให้บริการต้องดำเนินการแจ้งเตือนและให้คำแนะนำเมื่อเกิดเหตุการณ์ภัยคุกคาม ทั้งนี้ เกณฑ์ชี้วัดและเงื่อนไขในการจัดระดับความรุนแรงที่แน่ชัด อย่าง การประเมินผลกระทบทางธุรกิจ การอ้างอิงคะแนนความรุนแรงของช่องโหว่ (CVSS/CVE) และการกำหนดเงื่อนไขใน Playbook **ผู้ให้บริการต้องร่วมกับทาง สขญ. ในการร่างข้อกำหนดในช่วงของขั้นตอนการติดตั้งและเตรียมระบบ** เพื่อให้เหมาะสมกับสภาพแวดล้อมจริงของ สขญ. โดยให้ถือว่าข้อระดับความรุนแรงและระยะเวลาการตอบสนองดังต่อไปนี้ เป็นขั้นต่ำ

4.2.4.1 ระดับวิกฤต (Critical): ระยะเวลาแจ้งเตือนให้ สขญ. รับทราบ ภายใน 15 นาที และระยะเวลาให้คำแนะนำหรือตอบสนองต่อเหตุ ภายใน 1 ชั่วโมง

4.2.4.2 ระดับสูง (High): ระยะเวลาแจ้งเตือนให้ สขญ. รับทราบ ภายใน 1 ชั่วโมง และระยะเวลาให้คำแนะนำหรือตอบสนองต่อเหตุ: ภายใน 2 ชั่วโมง

4.2.4.3 ระดับปานกลาง (Medium): ระยะเวลาแจ้งเตือนให้ สขญ. รับทราบ ภายใน 2 ชั่วโมง และ ระยะเวลาให้คำแนะนำหรือตอบสนองต่อเหตุ ภายใน 24 ชั่วโมง

4.2.4.4 ระดับต่ำ (Low): ระยะเวลาแจ้งเตือนให้ สขญ. รับทราบ ภายใน 12 ชั่วโมง และระยะเวลาให้คำแนะนำหรือตอบสนองต่อเหตุตามความเหมาะสม

4.2.4.5 ระดับข้อมูล (Information): ระยะเวลาแจ้งเตือนให้ สขญ. รับทราบ ภายใน 24 ชั่วโมง และ ระยะเวลาให้คำแนะนำหรือตอบสนองต่อเหตุตามความเหมาะสม

4.2.5 ระบบบริหารจัดการเหตุการณ์และรูปแบบการแจ้งเตือน (Case Management & Notification)

4.2.5.1 ผู้ให้บริการต้องมีระบบ Incident Management หรือ Case Management ของตนเองสำหรับให้ สขญ. ใช้บันทึกประวัติ ติดตามสถานะเหตุการณ์ และใช้วัดผลตาม SLA ได้อย่างโปร่งใส

4.2.5.2 โดยข้อกำหนดการรายงานแจ้งเตือนเมื่อมีภัยคุกคามเกิดขึ้นในระบบ สขญ. จะต้องครอบคลุมเนื้อหาอย่างน้อย ต่อไปนี้

1. ชื่อการแจ้งเตือนที่ตรวจพบ (Rule Name)
2. วันและเวลาที่ตรวจพบ (Timestamp)
3. รายละเอียดของเหตุการณ์ พฤติกรรมการโจมตี และกฎที่ถูกละเมิด
4. ระดับความร้ายแรง: เช่น Critical, High, Medium, Low
5. ทรัพย์สินที่ได้รับผลกระทบ: เช่น IP Address, Hostname, ชื่อทรัพย์สิน, ผู้ใช้งาน
6. ระบุวิธีการแก้ไขหรือคำแนะนำสำหรับการแก้ไข: เช่น ลำดับสิ่งที่ต้องทำในการแก้ไขปัญหา ตั้งแต่ต้นจนจบ
7. ทางลัดหรือลิงก์ไปยังหน้า Dashboard และ Log ที่เกี่ยวข้อง
8. ช่องทางการติดต่อทีมสนับสนุนและบุคคลที่เกี่ยวข้อง

4.2.5.3 สำหรับการติดต่อสื่อสารทั่วไปสามารถใช้ อีเมล หรือแอปพลิเคชันที่ตกลงร่วมกันได้ แต่ในกรณีเกิดเหตุการณ์ระดับ Critical หรือ High **ผู้ให้บริการต้องดำเนินการ โทรศัพท์แจ้งเหตุโดยตรงร่วมด้วยเสมอ**

4.2.6 อำนาจในการจัดการระบบ SOAR ต่อเหตุการณ์เบื้องต้น (Incident Response Authority): เพื่อให้การระงับเหตุภัยคุกคามเป็นไปอย่างทันท่วงทีตามเงื่อนไข ข้อระดับความรุนแรงและระยะเวลาการตอบสนอง (SLA) สขญ. กำหนดขอบเขตอำนาจให้ผู้ให้บริการดำเนินการระงับเหตุผ่านระบบ SOAR หรือระบบอื่น ๆ โดยอ้างอิงตาม Playbook ที่ผ่านการอนุมัติแล้วเท่านั้น ดังนี้

4.2.6.1 การดำเนินการที่ **ไม่ต้องขออนุมัติล่วงหน้า**: ทันทีเมื่อตรวจพบเหตุการณ์ระดับวิกฤต (Critical) ผู้ให้บริการมีสิทธิ์ดำเนินการดังข้อต่อไปนี้ทันที โดยต้องบันทึกหลักฐานและรายงานให้ สขญ. ทราบภายใน 30 นาที

1. การแยกอุปกรณ์ปลายทางที่ต้องสงสัย (Isolation) ออกจากระบบเครือข่าย
2. การปิดกั้น IP Address หรือ Domain ที่เป็นแหล่งที่มาของภัยคุกคามในระดับอุปกรณ์เครือข่าย/Firewall
3. การระงับสิทธิ์การใช้งานบัญชีผู้ใช้ (Account Suspension) ที่ถูกบุกรุกชั่วคราว

4.2.6.2 การดำเนินการที่ **ต้องขออนุมัติล่วงหน้า**: ผู้ให้บริการต้องได้รับการอนุมัติจากเจ้าหน้าที่ของ สขญ. ก่อนดำเนินการ หรือปฏิบัติตามเงื่อนไขที่ตกลงกันไว้ใน Playbook หรือตามที่ สขญ. เห็นควร ในกรณีดังต่อไปนี้เป็นอย่างน้อย

1. การลบ แก้ไข หรือเปลี่ยนแปลงข้อมูลใด ๆ ในระบบของ สขญ.
2. การปิดกั้น IP Address ภายในองค์กรที่อาจส่งผลกระทบต่อการทำงาน
3. การดำเนินการใด ๆ ที่อาจส่งผลกระทบต่อความพร้อมใช้งานของระบบบริการหลัก

4.2.7 **บุคลากรสนับสนุน ณ ที่ทำการ (On-site Support)**

4.2.7.1 ผู้ให้บริการต้องจัดส่งบุคลากรที่มีความเชี่ยวชาญตั้งแต่ระดับตามข้อ 4.4.2 ขึ้นไป เข้ามาปฏิบัติงาน ณ ที่ทำการของ สขญ. เพื่อสนับสนุนการบริหารจัดการเหตุการณ์ ช่วยเหลือสืบสวน วิเคราะห์ หรือแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ ตามที่ สขญ. ร้องขอ ตลอดอายุสัญญา

4.2.8 **การรายงานผลการปฏิบัติงาน (Reporting & Delivery)**

4.2.8.1 รายงานรายวัน (Daily Report): ผู้ให้บริการต้องส่งสรุปเหตุการณ์ผิดปกติที่ตรวจพบและสถานะความปลอดภัยเบื้องต้นในแต่ละวัน

4.2.8.2 รายงานรายเดือน (Monthly Report): ผู้ให้บริการต้องจัดทำและส่งมอบรายงานภายใน 7 วันทำการของเดือนถัดไป โดยต้องมีเนื้อหาสรุปภาพรวมการปฏิบัติงานอย่างน้อยดังต่อไปนี้

1. สรุปภาพรวมการเฝ้าระวังและวิเคราะห์สถิติเหตุการณ์ภัยคุกคามที่เกิดขึ้นในรอบเดือน
2. สรุปประสิทธิภาพการทำงานและการตอบสนองเหตุการณ์เปรียบเทียบกับเกณฑ์ SLA ที่กำหนดไว้
3. สถานะความพร้อมใช้งานของระบบ (System Uptime): สรุปความพร้อมใช้งานของระบบ SIEM และเครื่องมือที่เกี่ยวข้อง เพื่อใช้เป็นข้อมูลอ้างอิงในการประเมินและคำนวณอัตราค่าปรับตามเงื่อนไขที่กำหนด

4. สรุปปริมาณข้อมูล Log และแหล่งที่มาของข้อมูล (Log Sources): ผู้ให้บริการต้องแสดงรายงานสรุปปริมาณข้อมูลทั้งหมดที่ระบบ SIEM ได้รับ พร้อมทั้งรายงานสถานะการใช้โควตาข้อมูล หรือยอดคงเหลือของปริมาณข้อมูลสำรองฉุกเฉิน (Volume Buffer) ประจำเดือน (หากมี) โดยทำการแจกแจงรายละเอียด ให้เห็นอย่างชัดเจนว่าข้อมูล Log ถูกส่งมาจากอุปกรณ์ ระบบ หรือสภาพแวดล้อมคลาวด์ใดบ้าง เช่น ระบบเครือข่าย, อุปกรณ์ปลายทาง, AWS, Microsoft Defender for Office 365 ฯลฯ พร้อมระบุสัดส่วนปริมาณข้อมูลของแต่ละแหล่งที่มา
5. ข้อเสนอแนะเชิงลึกในการปรับปรุงนโยบายความมั่นคงปลอดภัย หรือการปรับแต่งระบบให้มีประสิทธิภาพมากขึ้น

   แนวโน้มภัยคุกคามทางไซเบอร์: สรุปข้อมูลข่าวสาร แนวโน้มภัยคุกคามใหม่ ๆ หรือช่องโหว่สำคัญ (Zero-day Vulnerabilities) ที่ระดับสากลหรือในกลุ่มอุตสาหกรรมกำลังเผชิญ พร้อมประเมินความเสี่ยงและให้คำแนะนำในการเตรียมความพร้อมสำหรับ สขญ.

4.2.8.3 รายงานหลังเกิดเหตุการณ์ (Post-Incident Report): ผู้ให้บริการต้องจัดทำรายงานเมื่อเกิดเหตุภัยคุกคามระดับสูง (High) หรือระดับวิกฤต (Critical) หรือตามที่ สขญ. ร้องขอ โดยรูปแบบและข้อมูลภายในรายงานจะต้องครอบคลุมและสอดคล้องกับ แบบรายงานเอกสารใน ภาคผนวก เอกสาร ก1 และ เอกสาร ก2 เพื่อให้ สขญ. สามารถนำข้อมูลไปใช้รายงานต่อหน่วยงานภาครัฐได้อย่างครบถ้วนทันที โดยผู้ให้บริการต้องระบุรายละเอียดข้อมูลอย่างน้อยดังต่อไปนี้

1. ข้อมูลการประเมินภัยคุกคามเบื้องต้น
   - ระบุระดับความรุนแรงของภัยคุกคามทางไซเบอร์ เช่น ไม่ร้ายแรง, ร้ายแรง, วิกฤต ตามมาตรฐานมาตรา 60
   - ระบุหมวดหมู่ของภัยคุกคาม เช่น Reconnaissance, Malicious Logic, Denial of Service เป็นต้น
2. ข้อมูลการตรวจพบและผลกระทบ
   - วันและเวลาที่เกิดเหตุ และเวลาที่ตรวจพบ
   - สถานที่ตั้ง ฮาร์ดแวร์ ซอฟต์แวร์ และเครือข่ายของระบบที่ได้รับผลกระทบ
3. รายละเอียดทางเทคนิคและการวิเคราะห์
   - หมายเลขช่องโหว่ (CVE) หรือเทคนิคที่ถูกใช้จู่โจม
   - อาการหรือสิ่งผิดปกติที่เกิดขึ้นกับระบบ เช่น ระบบล่ม, ตรวจพบ Traffic ผิดปกติ, การยกระดับสิทธิ์, ไฟล์ถูกแก้ไข
   - ตัวบ่งชี้การโจมตี (IOA) และตัวบ่งชี้การบุกรุก (IOC)
   - แผนภาพและรายละเอียดเหตุการณ์ตามลำดับเวลา (Timeline) ตั้งแต่การจู่โจมครั้งแรกจนถึงปัจจุบัน

4. ข้อมูลการรับมือ ฟื้นฟู และแก้ไข (Response & Recovery)
    - สถานะการรับมือและสิ่งที่ได้ดำเนินการแก้ไขไปแล้ว เช่น การ Isolate ระบบ, ตรวจสอบ Log
    - การคาดการณ์ความสามารถและระยะเวลาในการฟื้นฟูระบบ
5. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (Post-Incident Activities)
    - วันและเวลาที่เหตุภัยคุกคามสิ้นสุด
    - การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกันในอนาคต
    - การวิเคราะห์ต้นเหตุ และบทเรียนที่ได้รับ (Lessons Learned)
6. หลักฐานประกอบ: ผู้ให้บริการต้องแนบข้อมูลจราจรคอมพิวเตอร์ (Log files) ทั้งหมดที่เกี่ยวข้องกับเหตุการณ์ส่งมอบให้ทาง สขญ. ร่วมด้วย

4.2.8.4 รายงานสรุปภัยคุกคามทางไซเบอร์: ผู้ให้บริการต้องจัดทำรายงานตามที่ สขญ.ขอ โดยรูปแบบและข้อมูลภายในรายงานจะต้องครอบคลุมและสอดคล้องกับแบบรายงานเอกสารใน ภาคผนวก ก3 เพื่อให้ สขญ. สามารถนำข้อมูลไปใช้รายงานต่อหน่วยงานภาครัฐได้อย่างครบถ้วนทันที โดยผู้ให้บริการต้องระบุรายละเอียดข้อมูลอย่างน้อยดังต่อไปนี้

1. สถิติจำแนกตาม หมวดหมู่ของภัยคุกคาม เช่น การพยายามบุกรุก การใช้มัลแวร์ การทำให้ปฏิเสธการให้บริการ
2. สถิติจำแนกตาม ทรัพย์สินที่ได้รับผลกระทบ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เว็บไซต์
3. สถิติจำแนกตาม ระดับภัยคุกคามทางไซเบอร์ อย่าง ไม่ร้ายแรง ร้ายแรง วิกฤต

4.3 **ขอบเขตการติดตั้ง**

ผู้ให้บริการต้องดำเนินการติดตั้ง เชื่อมต่อระบบ และจัดทำเอกสารมาตรฐานให้พร้อมสำหรับการให้บริการศูนย์ปฏิบัติการ SOC และเพื่อรองรับการขยายผลหรือการบริหารจัดการด้วยตนเอง ในอนาคต ภายในงวดที่ 1 โดยมีรายละเอียดขอบเขตการดำเนินงานดังต่อไปนี้

4.3.1 **การดำเนินการติดตั้งบนสภาพแวดล้อมหลัก**

ผู้ให้บริการต้องดำเนินการติดตั้งระบบบนสภาพแวดล้อม Cloud หรือ On-premises ตามที่ สขญ. กำหนด โดย สขญ. จะเป็นผู้จัดสรรทรัพยากรพื้นฐาน เช่น Virtual Machine, Tenant หรือมอบสิทธิ์การเข้าถึงที่จำเป็นให้แก่ผู้ให้บริการดำเนินการ ทั้งนี้ ผู้ให้บริการต้องรับผิดชอบงานดังต่อไปนี้

4.3.1.1 การติดตั้งและรวบรวม Log: ดำเนินการติดตั้งระบบ อุปกรณ์ Agent หรือซอฟต์แวร์ที่เกี่ยวข้อง เช่น SIEM, Log Forwarder ลงในสภาพแวดล้อมของ สขญ.

4.3.1.2 การบูรณาการระบบ (System Integration): ดำเนินการตั้งค่าการเชื่อมต่อ เพื่อรวบรวม Log และทำงานร่วมกับอุปกรณ์รักษาความปลอดภัยอื่นๆ ได้อย่างสมบูรณ์แบบ เพื่อให้สามารถดึงข้อมูลและสั่งการตอบสนองได้ โดยไม่มีการคิดค่าใช้จ่ายในการพัฒนาเพิ่มเติม

4.3.1.3 การตั้งค่าการตรวจจับ: ดำเนินการสร้างเงื่อนไขการตรวจจับ (Use cases/Correlation Rules) และตั้งค่าการแจ้งเตือนภัยคุกคามให้สอดคล้องกับระดับ SLA ที่กำหนด

4.3.2 **การจัดทำเอกสารแม่แบบ และคู่มือสำหรับการขยายระบบในอนาคต**

สำหรับการเชื่อมต่อระบบ โครงการ หรือ Cloud อื่น ๆ ที่อาจเพิ่มขึ้นในอนาคต สขญ. อาจเป็นผู้ดำเนินการติดตั้งด้วยตนเองเพื่อความคล่องตัว โดยผู้ให้บริการจะต้องส่งมอบสิ่งต่อไปนี้

4.3.2.1 จัดทำเอกสาร แม่แบบการตั้งค่า (Configuration Templates) มาตรฐาน สำหรับระบบปฏิบัติการหรือ Cloud ที่รองรับ

4.3.2.2 จัดทำเอกสาร คู่มือการติดตั้ง และ คู่มือการถอนการติดตั้ง ที่มีละเอียดและเข้าใจง่าย

4.3.2.3 ทั้งนี้ เมื่อ สขญ. ดำเนินการเพิ่มระบบหรือเชื่อมต่อโครงการใหม่เข้าสู่ศูนย์ SOC ด้วยตนเองตามคู่มือดังกล่าว จะไม่มีการคิดค่าใช้จ่ายในส่วนของบริการติดตั้งเพิ่มเติม โดยผู้ให้บริการจะคิดค่าบริการเฉพาะตามปริมาณข้อมูล (Log Volume) ที่ใช้งานจริง ซึ่งต้องไม่เกินข้อกำหนดที่ระบุไว้ในสัญญาเท่านั้น

4.3.3 **การส่งมอบ Blueprint ระบบ (System Blueprint Requirement)**

เพื่อเตรียมความพร้อมสู่การบริหารจัดการศูนย์ SOC ด้วยตนเองของ สขญ. ในอนาคต เมื่อดำเนินโครงการแล้วเสร็จ หรือตามช่วงเวลาที่ สขญ. กำหนด ผู้ให้บริการจะต้องส่งมอบข้อมูลระบบดังต่อไปนี้

4.3.3.1 เอกสารสถาปัตยกรรมระบบ รวมถึงรายการซื่อซอฟต์แวร์ ลิขสิทธิ์ หรือระบบโอเพนซอร์สที่ใช้ในการทำงานทั้งหมด

4.3.3.2 ส่งมอบ Source Code ของ Script โครงสร้างชุดกฎเกณฑ์การตรวจจับ (Correlation Rules) ที่ปรับแต่งสำหรับ สขญ. และกระบวนการของ Playbook ทั้งหมด โดยต้องส่งมอบในรูปแบบที่สามารถอ่านหรือนำไปปรับใช้งานต่อได้

4.3.4 **การจัดทำห่วงโซ่การแจ้งเตือนและยกระดับเหตุการณ์ (Escalation Matrix)**

ผู้ให้บริการต้องส่งมอบข้อกำหนดห่วงโซ่การแจ้งเตือนให้ สขญ. อนุมัติ เพื่อใช้เป็นมาตรฐานในการปฏิบัติงานจริง โดยต้องระบุรายละเอียดอย่างน้อยดังนี้

4.3.4.1 โครงสร้างการติดต่อ: รายชื่อ ตำแหน่ง โทรศัพท์ และอีเมล ของผู้รับผิดชอบในแต่ละระดับ (ทั้งฝั่งผู้ให้บริการและ สขญ.) โดยต้องปรับปรุงข้อมูลภายใน 7วัน ทุกครั้งที่มีการเปลี่ยนแปลงบุคลากร

4.3.4.2 เงื่อนไขการยกระดับ (Escalation Path): ลำดับขั้นการส่งต่อปัญหา เช่น L1 ⟶ L2 ⟶ L3 ⟶ ผู้บัญชาการเหตุการณ์ และระยะเวลาสูงสุด ก่อนยกระดับไปยังขั้นถัดไป

4.3.4.3 เงื่อนไขเวลาทำงาน: กำหนดกระบวนการส่งต่อเหตุการณ์ให้เจ้าหน้าที่ สขญ. รับทราบหรือร่วมตัดสินใจเฉพาะในเวลาทำการปกติของภาครัฐ (8x5) ยกเว้น เหตุการณ์ระดับ Critical หรือ High ที่ต้องดำเนินการทันที ให้มีกระบวนการโทรศัพท์แจ้งเตือนผู้ประสานงานที่กำหนดของ สขญ. นอกเวลาทำการได้ตลอด 24 ชั่วโมง

4.3.5 **การจัดทำและขออนุมัติเอกสารการตอบโต้ภัยคุกคาม (Incident Playbooks)**

ผู้ให้บริการต้องดำเนินการจัดทำคู่มือกระบวนการตอบสนองต่อเหตุการณ์ภัยคุกคามรูปแบบต่างๆ จำนวนไม่น้อยกว่า 5 รูปแบบ เช่น Malware, Phishing, Unauthorized Access, Data Exfiltration ให้สอดคล้องกับระบบและบริบทการทำงานของ สขญ. โดยมีเงื่อนไขดังนี้

4.3.5.1 การกำหนดเงื่อนไขและขั้นตอนใน Playbook ที่เกี่ยวข้องกับ อำนาจในการจัดการระบบ และการตั้งค่าให้ระบบตอบสนองแบบอัตโนมัติ (Automated Response) **จะต้องผ่านการตรวจสอบและรับรองจากทาง สขญ. ก่อนนำไปใช้งานจริงบนระบบเสมอ**

4.3.5.2 ผู้ให้บริการจะต้องดำเนินการจัดทำและปรับปรุง Playbook รูปแบบใหม่ ๆ เพิ่มเติมตามความเสี่ยงใหม่ที่ตรวจพบ หรือตามที่ สขญ. ร้องขอตลอดระยะเวลาสัญญา โดยไม่จำกัดจำนวน และไม่คิดค่าใช้จ่ายเพิ่มเติมใด ๆ ทั้งสิ้น

4.4 **ข้อกำหนด บุคลากรประจำศูนย์ฯ**

ที่ปฏิบัติงานภายใต้โครงการนี้ **จะต้องเป็นสัญชาติไทยทั้งหมด** เพื่อความมั่นคงของชาติและความปลอดภัยของข้อมูล โดยผู้ให้บริการต้องจัดให้มีบุคลากรที่มีคุณสมบัติขั้นต่ำ ดังนี้

4.4.1 **ผู้ปฏิบัติงานขั้นต้น (Level 1 Incident Analyst)** ประจำ โดยมีคุณสมบัติขั้นต่ำดังนี้

4.4.1.1 สำเร็จการศึกษาระดับปริญญาตรีด้านวิศวกรรมคอมพิวเตอร์ วิทยาศาสตร์คอมพิวเตอร์ หรือสาขาอื่นที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศเป็นอย่างน้อย

4.4.1.2 สามารถใช้งานระบบเฝ้าระวังความมั่นคงปลอดภัยทางคอมพิวเตอร์ระบบปัจจุบันของ สขญ. ได้เป็นอย่างดี

4.4.1.3 มีประสบการณ์ทำงานหรือได้รับการอบรมทางด้านความมั่นคงปลอดภัย สารสนเทศ

4.4.2 **ผู้ปฏิบัติงานขั้นกลาง (Level 2 Incident Analyst)** ประจำ โดยมีคุณสมบัติขั้นต่ำดังนี้

4.4.2.1 สำเร็จการศึกษาระดับปริญญาตรีด้านวิศวกรรมคอมพิวเตอร์ วิทยาศาสตร์คอมพิวเตอร์ หรือสาขาอื่นที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศเป็นอย่างน้อย

4.4.2.2 สามารถใช้งานระบบเฝ้าระวังความมั่นคงปลอดภัยทางคอมพิวเตอร์ระบบปัจจุบันของ สขญ. ได้เป็นอย่างดี

4.4.2.3 สามารถให้คำปรึกษาและคำแนะนำเบื้องต้นในการแก้ไขปัญหาด้านความมั่นคงปลอดภัยสารสนเทศได้

4.4.2.4 มีประสบการณ์ทำงานด้านความมั่นคงปลอดภัยสารสนเทศอย่างน้อย 1 ปี

4.4.3 **ผู้ปฏิบัติงานระดับหัวหน้าศูนย์ (CSOC Leader)** ประจำ โดยมีคุณสมบัติขั้นต่ำดังนี้

4.4.3.1 จบการศึกษาระดับปริญญาโท หรือสูงกว่าในสาขา เทคโนโลยีสารสนเทศ วิศวกรรมคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้องเป็นอย่างน้อย

4.4.3.2 มีประสบการณ์ทำงานด้านความมั่นคงปลอดภัยสารสนเทศอย่างน้อย 4 ปี

4.5 **เงื่อนไขอื่น ๆ**

4.5.1 ความรับผิดชอบด้านค่าใช้จ่ายที่เกี่ยวข้องกับระบบและการรับส่งข้อมูล

เพื่อให้การบริการศูนย์ปฏิบัติการ SOC เป็นไปอย่างสมบูรณ์ ผู้ให้บริการจะต้องเป็นผู้รับผิดชอบค่าใช้จ่ายที่เกิดขึ้นในส่วนของระบบผู้ให้บริการอย่างครบถ้วน โดยมีเงื่อนไขดังต่อไปนี้

4.5.1.1 ค่าใช้จ่ายฝั่งระบบของผู้ให้บริการ: ผู้ให้บริการต้องรับผิดชอบค่าใช้จ่ายทั้งหมดที่เกิดขึ้นบนโครงสร้างพื้นฐานของผู้ให้บริการ เช่น ค่า Cloud Infrastructure ของระบบ SIEM/SOC ค่า Inbound/Outbound Traffic ขาเข้าและขาออกจากระบบ

ของผู้ให้บริการ ค่าลิขสิทธิ์ซอฟต์แวร์ และค่าการเข้าถึงหน้า Dashboard โดย สขญ. จะไม่มีการจ่ายค่าบริการส่วนเพิ่มใดๆ ทั้งสิ้นในส่วนนี้

4.5.1.2 ค่าใช้จ่ายในการขอข้อมูลหลักฐานจากระบบ: ในกรณีเกิดเหตุการณ์ภัยคุกคาม และ สขญ. มีความจำเป็นต้องร้องขอข้อมูลจากระบบที่ผู้ให้บริการดูแล เพื่อใช้เป็นพยานหลักฐาน เช่น ข้อมูลจราจรคอมพิวเตอร์ (Log Files) หรือข้อมูลบันทึกแพ็กเก็ตเครือข่าย (PCAP) ผู้ให้บริการจะต้องจัดเตรียมและส่งมอบข้อมูลดังกล่าวผ่านช่องทางที่ปลอดภัย โดยถือเป็นส่วนหนึ่งของบริการและไม่คิดค่าใช้จ่ายเพิ่มเติมใด ๆ ทั้งสิ้นจาก สขญ.

4.5.1.3 ข้อกำหนดด้านสถาปัตยกรรมเพื่อลดภาระค่าใช้จ่ายของ สขญ.: ในการออกแบบสถาปัตยกรรมการส่งข้อมูล จากระบบต้นทางของ สขญ. ไปยังระบบของผู้ให้บริการ ผู้ให้บริการจะต้องออกแบบวิธีการส่งข้อมูลที่**ประหยัดและมีประสิทธิภาพสูงสุด** เช่น การบีบอัดข้อมูลก่อนส่งมอบ หรือการตั้ง Log Collector ภายในเครือข่ายของ สขญ. เพื่อลดภาระค่าใช้จ่าย Data Transfer Out (Egress Cost) บนระบบ Cloud ของ สขญ. ให้เหลือน้อยที่สุด

5. กำหนดระยะเวลาส่งมอบพัสดุ และระยะเวลาดำเนินการให้บริการ

กำหนดส่งมอบงานภายใน 60 วันนับถัดจากวันลงนามในสัญญา โดยมีระยะเวลาใช้งาน 22 เดือน เริ่มตั้งแต่วันที่ 1 พฤศจิกายน 2569 - 31 สิงหาคม 2571

6. วงเงินงบประมาณ

งบประมาณประจำปี 2569 เป็นเงินจำนวน 3,165,079.00 บาท (สามล้านหนึ่งแสนหกหมื่นห้าพันเจ็ดสิบเก้าบาทถ้วน) รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงด้วยแล้ว

7. งวดงานและการจ่ายเงิน

การส่งมอบงานและการจ่ายเงินค่าบริการ แบ่งออกเป็น 23 งวด โดยมีรายละเอียดดังต่อไปนี้

7.1 **งวดที่ 1** การติดตั้ง เตรียมความพร้อม และเริ่มให้บริการ (Setup & Onboarding): ผู้ให้บริการจะต้องส่งมอบงานภายใน 60 วัน นับถัดจากวันที่ลงนามในสัญญา โดยกำหนดจ่ายเงินคิดเป็น ร้อยละ 20 ของมูลค่าสัญญา เมื่อผู้ให้บริการได้ดำเนินงานติดตั้งระบบและเตรียมความพร้อม ตามข้อ 4.3 แล้วเสร็จ และทำหนังสือส่งมอบงานงวดที่ 1 จำนวน 1 ชุด โดยคณะกรรมการได้ทำการตรวจรับเรียบร้อยแล้ว ซึ่งมีรายละเอียดผลส่งมอบดังต่อไปนี้:

7.1.1 แผนการดำเนินโครงการ (Project Plan) ในรูปแบบ Gantt Chart

7.1.2 รายงานผลการติดตั้งและบูรณาการระบบ (System Integration Report) ที่แสดงว่าระบบ SIEM สามารถรับ Log จากระบบของ สขญ. ได้ครบถ้วนตามขอบเขต

7.1.3 เอกสารสถาปัตยกรรมระบบ (Architecture Diagram) และคู่มือการติดตั้งเบื้องต้น

7.1.4 เอกสารกำหนดห่วงโซ่การแจ้งเตือนและยกระดับเหตุการณ์ (Escalation Matrix)

7.1.5 คู่มือกระบวนการตอบสนองต่อเหตุการณ์ภัยคุกคาม (Incident Playbooks) จำนวนไม่น้อยกว่า 5 รูปแบบ ที่ผ่านการอนุมัติจาก สขญ.

7.1.6 รายงานผลการทดสอบระบบ เพื่อยืนยันความพร้อมในการเฝ้าระวังภัยคุกคามตลอด 24 ชั่วโมง

7.1.7 รายงานสรุปผลการปฏิบัติงานรายเดือน (Monthly Report) สำหรับช่วงเดือนที่เริ่มเปิดให้บริการ

7.2 **งวดที่ 2 ถึง งวดที่ 20 และ งวดที่ 22** กำหนดจ่ายเงินค่าบริการ ร้อยละ 3.5 ของมูลค่าสัญญา พร้อมทำหนังสือส่งมอบงานแต่ละงวด จำนวน 1 ชุด โดยคณะกรรมการได้ทำการตรวจรับเรียบร้อยแล้ว

7.3 **งวดที่ 21** กำหนดจ่ายเงินค่าบริการ ร้อยละ 4 ของมูลค่าสัญญา เมื่อผู้ให้บริการได้ดำเนินการครบถ้วนดังข้อ 4.2 พร้อมทำหนังสือส่งมอบงานแต่ละงวด จำนวน 1 ชุด โดยคณะกรรมการได้ทำการตรวจรับเรียบร้อยแล้ว

7.3.1.1 ผู้ให้บริการต้องจัดทำและนำเสนอแผนการถ่ายโอนงาน และให้ความร่วมมืออย่างเต็มที่ในการถ่ายทอดข้อมูล กฎเกณฑ์การตรวจจับ และการตั้งค่าทั้งหมด คืนให้แก่ สขญ. หรือผู้ให้บริการรายใหม่ โดยระบบจะต้องสามารถให้บริการได้อย่างต่อเนื่องจนกว่าจะสิ้นสุดสัญญา โดยไม่คิดค่าใช้จ่ายเพิ่มเติม

7.4 **งวดที่ 23** กำหนดจ่ายเงินค่าบริการงวดสุดท้าย ร้อยละ 6 ของมูลค่าสัญญา โดยผู้ให้บริการต้องส่งมอบงานภายใน 7 วันทำการของเดือนถัดไป หรือตามวันสิ้นสุดสัญญา และทำหนังสือส่งมอบงานงวดสุดท้าย จำนวน 1 ชุด โดยมีรายละเอียดผลส่งมอบดังต่อไปนี้:

7.4.1 รายงานผลการปฏิบัติงานรายเดือน (Monthly Report) ของเดือนสุดท้าย

7.4.2 รายงานสรุปผลการดำเนินงานรวมตลอดโครงการ

7.4.3 เอกสารและรายงานผลการส่งมอบงานเมื่อสิ้นสุดสัญญา รวมถึงการส่งมอบโครงสร้างชุดกฎเกณฑ์การตรวจจับ (Correlation Rules) ล่าสุดคืนให้แก่ สขญ.

7.4.4 หนังสือรับรองการทำลายข้อมูล ในกรณีที่ สขญ. ไม่ต่อสัญญาและแจ้งให้ดำเนินการลบข้อมูลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

8. อัตราค่าปรับ

8.1 หากผู้ให้บริการไม่สามารถทำงานให้แล้วเสร็จตามเวลาที่กำหนดไว้ในสัญญา ผู้ให้บริการจะต้องชำระค่าปรับให้แก่ สถาบันฯ เป็นรายวันในอัตราร้อยละ 0.10 (ศูนย์จุดหนึ่งศูนย์) ของมูลค่าสัญญาจ้าง แต่จะต้องไม่ต่ำกว่าวันละ 100 บาท

8.2 กรณีผู้ให้บริการไม่ปฏิบัติให้เป็นไปตามระดับการให้บริการ (Service Level Agreement : SLA) ในการให้บริการศูนย์ SOC หากผู้ให้บริการไม่สามารถแจ้งเตือน วิเคราะห์ ให้คำแนะนำ หรือดำเนินการแก้ไขเหตุการณ์ภัยคุกคามให้เป็นไปตามระยะเวลาที่กำหนดใน SLA ข้อ 4.2.4 ทาง สขญ. มีสิทธิหักค่าบริการจากเงินค่าจ้างในงวดเดือนนั้น โดยมีอัตราดังนี้

8.2.1 กรณีเหตุการณ์ระดับวิกฤต (Critical) หรือระดับสูง (High) หากผู้ให้บริการดำเนินการล่าช้ากว่าระยะเวลาที่กำหนดตาม SLA ผู้ว่าจ้างมีสิทธิหักค่าบริการจากเงินค่าจ้างในงวดเดือนนั้น ในอัตรา 500 บาทต่อเหตุการณ์ และในอัตรา 500 บาทต่อชั่วโมงสำหรับระยะเวลาที่ล่าช้าเกินกำหนด (โดยเศษของชั่วโมงให้นับเป็นหนึ่งชั่วโมง)

8.2.2 กรณีเหตุการณ์ระดับปานกลาง (Medium) หรือระดับต่ำ (Low) หากผู้ให้บริการดำเนินการล่าช้ากว่าระยะเวลาที่กำหนดตาม SLA ผู้ว่าจ้างมีสิทธิหักค่าบริการจากเงินค่าจ้างในงวดเดือน

นั้น ในอัตรา 200 บาทต่อเหตุการณ์ และในอัตรา 200 บาทต่อชั่วโมง สำหรับระยะเวลาที่ล่าช้าเกินกำหนด (โดยเศษของชั่วโมงให้นับเป็นหนึ่งชั่วโมง)

8.3 กรณีระบบความมั่นคงปลอดภัยไม่พร้อมใช้งาน (System Uptime) ระบบบริหารจัดการเหตุการณ์ (SIEM) และหน้าจอแสดงผล (Dashboard) ผู้ให้บริการต้องให้บริการมีความพร้อมใช้งานไม่น้อยกว่าร้อยละ 99.5 ต่อเดือน หากความพร้อมใช้งานต่ำกว่าที่กำหนด สขญ. มีสิทธิหักค่าบริการจากเงินค่าจ้างในงวดเดือนนั้น ในอัตรา 500 บาทต่อชั่วโมง สำหรับระยะเวลาที่ระบบไม่พร้อมใช้งาน (โดยเศษของชั่วโมงให้นับเป็นหนึ่งชั่วโมง)

8.4 กรณีระบบความมั่นคงปลอดภัยไม่พร้อมใช้งาน (System Uptime) ระบบบริหารจัดการเหตุการณ์ (SIEM) และหน้าจอแสดงผล (Dashboard) ของผู้ให้บริการ จะต้องมีความพร้อมใช้งาน ไม่น้อยกว่าร้อยละ 99.5 ต่อเดือน หากความพร้อมใช้งานต่ำกว่าเกณฑ์ดังกล่าว สขญ. จะทำการปรับหรือหักค่าบริการรายเดือนในอัตรา 500 บาท ต่อทุกๆ 1 ชั่วโมงที่ระบบไม่สามารถใช้งานได้

9. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

9.1 ในการพิจารณาผลการยื่นข้อเสนอครั้งนี้ สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) จะพิจารณาตัดสินโดยใช้หลักเกณฑ์ ราคาประกอบเกณฑ์อื่น

9.2 ผู้ให้บริการมีหน้าที่จัดทำข้อเสนอ ทางเทคนิคที่สอดคล้องกับขอบเขตการดำเนินงาน และข้อเสนอเพิ่มเติมของผู้ขายเพื่อให้งานมีความสมบูรณ์ โดยถือว่าข้อเสนอที่ผู้ขายเสนอนั้นอยู่ในขอบเขตค่าใช้จ่ายที่ได้กำหนดไว้แล้ว และจะไม่คิดค่าใช้จ่ายเพิ่มเติม

9.3 ผู้ให้บริการจะต้องมานำเสนอข้อเสนอ แผนการดำเนินงาน รายละเอียดผลงานกิจกรรมทางเทคนิคด้วยวาจาต่อคณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ ตามวันและเวลาที่สถาบันกำหนด ในเอกสารประกาศเชิญชวน รายละไม่เกิน 30 นาที และตอบข้อซักถาม 30 นาที

9.4 การพิจารณาผู้ชนะการยื่นข้อเสนอ กรณีใช้หลักเกณฑ์ราคาประกอบเกณฑ์อื่น ในการพิจารณาผู้ชนะการยื่นข้อเสนอสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) จะพิจารณาโดยให้คะแนนตามปัจจัยหลักและน้ำหนักที่กำหนด ดังนี้

1. ราคาที่ยื่นข้อเสนอ (price) กำหนดน้ำหนักเท่ากับ ร้อยละ 20
2. ข้อเสนอด้านเทคนิค กำหนดค่าน้ำหนักเท่ากับ ร้อยละ 80

วิธีการประเมินและให้คะแนน

9.4.1 รูปแบบการบริหารโควตาข้อมูล (คะแนนเต็ม 100 คะแนน) (น้ำหนักร้อยละ 15)

เกณฑ์การพิจารณา	คะแนน	วิธีการประเมิน
นำเสนอรูปแบบคิดค่าบริการแบบ ไม่จำกัดปริมาณข้อมูล โดยอ้างอิงขีดความสามารถในการประมวลผลไม่น้อยกว่า 1,000 Endpoint ต่อเดือน ซึ่งสามารถป้องกันปัญหาข้อมูลสูญหายจากสภาวะข้อมูลพุ่งสูง(Burst Volume) ได้อย่างสมบูรณ์แบบ	100	ประเมินจากเอกสารข้อเสนอทางเทคนิค และเอกสารคุณลักษณะของระบบ (Datasheet) ระบุเงื่อนไขการคิดโควตาและการยืดหยุ่นของข้อมูล หรือ รูปแบบการคิด License แบบ Endpoint และไม่จำกัดปริมาณการรับข้อมูล (Unlimited Ingestion) อย่างชัดเจน
นำเสนอรูปแบบคิดค่าบริการตามปริมาณข้อมูล (GB/Day) แบบมีเงื่อนไขยืดหยุ่น เช่น สามารถทบยอดสะสมได้ (Rollover/Token) หรือ ถัวเฉลี่ยรายเดือนร่วมกับมีกระเป๋าข้อมูลสำรอง (Volume Buffer) ให้โดยไม่คิดค่าใช้จ่ายเพิ่ม	80	

นำเสนอรูปแบบคิดค่าบริการตามปริมาณข้อมูล (GB/Day) แบบโควตาคงที่รายวัน (Fixed) ตัดรอบวันต่อวัน และไม่สามารถทบยอดคงเหลือได้ (Use it or lose it)	60	
ไม่นำเสนอรูปแบบการคิดค่าบริการ หรือรายละเอียดไม่ชัดเจน	0	

9.4.2 การจำแนกและบริหารโควตาข้อมูลระบบ SIEM (คะแนนเต็ม 100 คะแนน) (น้ำหนักร้อยละ 10)

เกณฑ์การพิจารณา	คะแนน	วิธีการประเมิน
ระบบสามารถจำแนกประเภทและแยกการบริหารจัดการข้อมูลได้อย่างอิสระ (เช่น แยกแยะ Log สำหรับ Active Monitoring ออกจาก Log สำหรับ Retention) **และ มีการเสนอโควตาข้อมูล เพิ่มเติมให้ฟรีมากกว่าเกณฑ์ขั้นต่ำ**ซึ่งคณะกรรมการพิจารณาแล้วเห็นว่าเป็นประโยชน์ต่อ สขญ. หรือ **เสนอรูปแบบไม่จำกัดปริมาณข้อมูล** (Unlimited Log)	100	ประเมินจากเอกสารข้อเสนอทางเทคนิค สถาปัตยกรรมระบบ และตารางสรุปโควตาพื้นที่การจัดเก็บที่นำเสนอ
ระบบสามารถจำแนกประเภทและแยกการบริหารจัดการข้อมูลได้อย่างอิสระ โดยสามารถกำหนดสัดส่วนหรือจำกัดอัตราข้อมูล (Rate Limiting / Quota Allocation) และสามารถคำนวณหรือควบคุมปริมาณข้อมูลได้ครบถ้วน **ทั้งที่อุปกรณ์ต้นทาง (Log Source) และระบบปลายทาง (SIEM)**	80	
ระบบสามารถจำแนกประเภทหรือ**คัดกรองข้อมูลได้เฉพาะที่อุปกรณ์ต้นทาง (Log Source) เท่านั้น** แต่ไม่สามารถแยกการบริหารจัดการโควตาอย่างอิสระเมื่อข้อมูลถูกส่งมาถึงระบบปลายทาง (SIEM) ได้	60	
ไม่สามารถจำแนกประเภทและบริหารจัดการโควตาข้อมูลได้ทั้งระบบต้นทางและปลายทาง หรือ เสนอพื้นที่พอดีตามเกณฑ์ขั้นต่ำโดยไม่มีความสามารถในการบริหารจำแนกดังกล่าว	0	

9.4.3 ระบบปัญญาประดิษฐ์ (AI Support) (คะแนนเต็ม 100 คะแนน) (น้ำหนักร้อยละ 10)

1. ด้านการค้นหาข้อมูล (Natural Language to Query): ระบบรองรับการใช้คำสั่งด้วยภาษามนุษย์ (Natural Language) เพื่อให้ AI แปลงเป็นคำสั่งค้นหาข้อมูล (Query Language) ในการสืบสวน Log หรือภัยคุกคามในระบบได้อย่างรวดเร็ว

2. ด้านการสรุปเหตุการณ์ (Incident & Timeline Summarization): ระบบมี AI ที่สามารถวิเคราะห์ สรุปความเชื่อมโยง และร้อยเรียงลำดับเหตุการณ์การโจมตี (Kill Chain/Timeline) จาก Alert ที่กระจัดกระจาย ให้ออกมาเป็นข้อความหรือรายงานที่มนุษย์เข้าใจได้ง่าย โดยอัตโนมัติ

3. ด้านการให้บริบทและคำแนะนำ (Knowledge Base): ระบบมี AI ที่ช่วยสรุปบริบทของภัยคุกคาม โดยอ้างอิงจากฐานข้อมูลภัยคุกคามสากล พร้อมทั้งสามารถให้คำแนะนำเชิงลึก หรือสร้างองค์ความรู้ (Knowledge Base) ถึงขั้นตอนการรับมือและแก้ไขปัญหาเบื้องต้นได้

เกณฑ์การพิจารณา	คะแนน	วิธีการประเมิน
มีเทคโนโลยี AI สนับสนุนการทำงาน ครบทั้ง 3 ด้าน	100	ประเมินจากเอกสารข้อเสนอทางเทคนิค, เอกสารคุณลักษณะของผลิตภัณฑ์ (Datasheet) หรือหลักฐานจากการสาธิตการทำงานของระบบ (POC) ที่สามารถแสดงผลการทำงานของ AI ตามที่ระบุได้จริง
มีเทคโนโลยี AI สนับสนุนการทำงาน จำนวน 2 ด้าน	80	
มีเทคโนโลยี AI สนับสนุนการทำงาน จำนวน 1 ด้าน	60	
ไม่มีเทคโนโลยี AI สนับสนุน หรือ มีแต่ไม่สามารถพิสูจน์การทำงานให้เห็นเป็นรูปธรรมได้ตามเกณฑ์ได้	0	

9.4.4 การเฝ้าระวัง Dark Web (Dark Web Monitoring) (คะแนนเต็ม 100 คะแนน) (น้ำหนักร้อยละ 10)

1. ด้านโดเมนและเครือข่าย (Domain & IP Address): สามารถตรวจสอบการรั่วไหล หรือการโจมตีที่เจาะจงมายังโดเมนเนม (Domain Name) และหมายเลขไอพี (IP Address) ของ สขญ. ได้
2. ด้านข้อมูลระบุตัวตน (Leaked Credentials): สามารถตรวจสอบและแจ้งเตือนการรั่วไหลของบัญชีผู้ใช้งาน อีเมล หรือรหัสผ่านของบุคลากร สขญ. ที่ถูกนำไปเผยแพร่หรือซื้อขายในตลาดมืดได้
3. ด้านคำค้นหาเฉพาะเจาะจง (Keywords & VIPs): สามารถตั้งค่าคำค้นหาอิสระ (Keywords) เช่น ชื่อหน่วยงาน, ชื่อระบบโครงการสำคัญ หรือชื่อผู้บริหารระดับสูง เพื่อเฝ้าระวังการถูกกล่าวถึงหรือวางแผนโจมตีได้

เกณฑ์การพิจารณา	คะแนน	วิธีการประเมิน
สามารถตรวจสอบและแจ้งเตือนการรั่วไหลแบบอัตโนมัติ โดยเจาะจงเป้าหมายได้ ครบทั้ง 3 ด้าน	100	ประเมินจากเอกสารข้อเสนอทางเทคนิค คุณลักษณะของระบบ หรือตัวอย่างการตั้งค่าระบบ
สามารถตรวจสอบและแจ้งเตือนการรั่วไหลแบบอัตโนมัติ โดยเจาะจงเป้าหมายได้ ครบทั้ง 2 ด้าน	80	
สามารถตรวจสอบและแจ้งเตือนการรั่วไหลแบบอัตโนมัติ โดยเจาะจงเป้าหมายได้ จำนวน 1 ด้าน หรือ **สามารถตรวจสอบได้แค่ระดับภัยคุกคามสากล** (Global Threat) โดยเจาะจงเป้าหมายไม่ได้	60	
ไม่มีความสามารถในการเฝ้าระวัง Dark Web	0	

9.4.5 ด้านคุณสมบัติและประสบการณ์ของบุคลากรปฏิบัติงานหลัก (คะแนนเต็ม 100 คะแนน) (น้ำหนักร้อยละ 10)

ผู้ให้บริการต้องนำเสนอบุคลากรหลัก โดยต้องเป็นบุคลากรที่ ไม่ซ้ำบุคคลกันจำนวนอย่างน้อย 2 ตำแหน่ง ดังนี้:

1. ผู้ปฏิบัติงานระดับหัวหน้าศูนย์ (CSOC Leader)
2. ผู้ปฏิบัติงานขั้นกลาง (Level-2 Incident Analyst)

เกณฑ์การพิจารณา	คะแนน	วิธีการประเมิน
ระดับดีเยี่ยม (Expert): - หัวหน้าศูนย์ฯ: **ประสบการณ์ทำงาน 10 ปีขึ้นไป** (พร้อมแนบใบรับรอง SEC+, CySA+ หรือ Pentest+ อย่างน้อย 1 รายการ) - ผู้ปฏิบัติงานขั้นกลาง (L2): **ประสบการณ์ทำงาน 5 ปีขึ้นไป** (พร้อมแนบใบรับรอง CEH หรือ CySA+ อย่างน้อย 1 รายการ)	100	ประเมินจากประวัติการทำงานและสำเนาใบรับรองมาตรฐานวิชาชีพสากล **ที่ยังไม่หมดอายุ** ณ วันที่ยื่นข้อเสนอ
ระดับดี (Professional): - หัวหน้าศูนย์ฯ: **ประสบการณ์ทำงานตั้งแต่ 5 ปีขึ้นไป** - ผู้ปฏิบัติงานขั้นกลาง (L2): **ประสบการณ์ทำงานตั้งแต่ 2 ปีขึ้นไป**	50	
ระดับผ่านเกณฑ์ขั้นต่ำ (Standard): บุคลากรมีประสบการณ์**ผ่านตามเกณฑ์ขั้นต่ำ**ที่กำหนดไว้	0	

9.4.6 ระดับการตอบสนองภัยคุกคามและการวิเคราะห์นิติวิทยาศาสตร์เชิงลึก (Advanced DFIR) (คะแนนเต็ม 100 คะแนน) (น้ำหนักร้อยละ 10)

ผู้ให้บริการจะต้องมีระบบการตอบสนองภัยคุกคามอัตโนมัติ (SOAR) และการจัดทำรายงานผ่านเกณฑ์มาตรฐ านขั้นต่ำตามที่ระบุในข้อกำหนดขอบเขตของงานเรียบร้อยแล้ว ทั้งนี้ คณะกรรมการจะพิจารณาให้คะแนนเพิ่มเติม จากขีดความสามารถด้านบริการนิติวิทยาศาสตร์ไซเบอร์ (Digital Forensics and Incident Response) ที่ผู้ให้บริการสามารถให้บริการเพิ่มเติมได้เมื่อเกิดเหตุการณ์วิกฤต โดยไม่มีค่าใช้จ่าย ซึ่งพิจารณาจากความสามารถ 3 ด้านหลัก ดังต่อไปนี้:

1. ด้านการตรวจพิสูจน์พยานหลักฐาน (Memory & Disk Forensics): การทำสำเนาและตรวจวิเคราะห์พยานหลักฐานทางดิ จิทัลระดับหน่วยความจำและฮาร์ดดิสก์
2. ด้านการวิเคราะห์มัลแวร์เชิงลึก (Malware Reverse Engineering): การวิเคราะห์ชำแหละรหัสสั่งการมัลแวร์
3. ด้านการรักษาสภาพหลักฐาน (Chain of Custody): กระบวนการรักษาสภาพพยานหลักฐานเพื่อรองรับการดำเนินคดีทางศาลและกฎหมาย

เกณฑ์การพิจารณา	คะแนน	วิธีการประเมิน
มีบริการทีมสืบสวนนิติวิทยาศาสตร์ไซเบอร์เชิงลึก (DFIR) ซึ่งมีขีดความสามารถครอบคลุม **ครบทั้ง 3 ด้าน**	100	ประเมินจากเอกสารข้อเสนอทางเทคนิค และขอบเขตการให้บริการที่ระบุขอบเขตบริการ DFIR **อย่างชัดเจน**
มีบริการสืบสวนเชิงลึก แต่ขีดความสามารถครอบคลุมเพียง **2 ด้าน** จากเกณฑ์ที่กำหนด	80	
มีบริการสืบสวนเชิงลึก แต่ขีดความสามารถครอบคลุมเพียง **1 ด้าน** จากเกณฑ์ที่กำหนด	60	
มีกระบวนการตอบสนองภัยคุกคามและการจัดทำรายงาน **ตามเกณฑ์มาตรฐานขั้นต่ำที่กำหนด**	0	

9.4.7 ข้อมูลภัยคุกคามเชิงลึก (Threat Intelligence) (คะแนนเต็ม 100 คะแนน) (น้ำหนักร้อยละ 5)

เกณฑ์การพิจารณา	คะแนน	วิธีการประเมิน
นำเสนอการเชื่อมต่อฐานข้อมูลภัยคุกคามแบบ ระดับพาณิชย์ (Commercial) ร่วมกับแหล่งข้อมูลแบบ Open Source	100	ประเมินจากเอกสารข้อเสนอทางเทคนิคและแผนการเชื่อมต่อระบบฐานข้อมูลภัยคุกคาม
นำเสนอการเชื่อมต่อเฉพาะฐานข้อมูลแบบ ระดับพาณิชย์ (Commercial) เท่านั้น	80	
นำเสนอการเชื่อมต่อเฉพาะฐานข้อมูลแบบ Open Source เท่านั้น	60	
ไม่การนำเสนอการเชื่อมต่อฐานข้อมูลภัยคุกคามเชิงลึกหรือรายละเอียดไม่ชัดเจน	0	

9.4.8 สถานที่จัดเก็บข้อมูล (คะแนนเต็ม 100 คะแนน) (น้ำหนักร้อยละ 5)

ผู้ให้บริการจะต้องผ่านเกณฑ์มาตรฐาน ขั้นต่ำด้านความมั่นคงปลอดภัย การเข้ารหัส และการปิดบังข้อมูล (Data Masking) ตามที่ระบุในข้อกำหนดเรียบร้อยแล้ว ทั้งนี้ คณะกรรมการจะพิจารณาให้คะแนนเพิ่มเติมหากผู้ให้บริการสามารถให้บริการระบบจัดเก็บข้อมูลที่ตั้งอยู่ภายในประเทศไทย เพื่อลดความเสี่ยงทางกฎหมายในการส่งข้อมูลออกนอกราชอาณาจักร (Cross-border Data Transfer)

เกณฑ์การพิจารณา	คะแนน	วิธีการประเมิน
จัดเก็บและประมวลผลข้อมูล Log ใน Data Center หรือ Cloud ที่**ตั้งอยู่ในประเทศไทยเท่านั้น** โดยอ้างอิงจากสำนักงานพัฒนารัฐบาลดิจิทัล (สพร.)	100	ประเมินจากเอกสารข้อเสนอทางเทคนิค และเอกสารรับรองสถานที่ตั้งและมาตรฐานของศูนย์ข้อมูล (Location & DGA Certification) ที่ยังไม่หมดอายุ
มีการจัดเก็บหรือส่งข้อมูลออกไปประมวลผล**ตามเกณฑ์มาตรฐานขั้นต่ำที่กำหนด**	0	

9.4.9 ความพร้อมของแผนงานและคู่มือ (Plan & Playbook) (คะแนนเต็ม 100 คะแนน) (น้ำหนักร้อยละ 5)

เกณฑ์การพิจารณา	คะแนน	วิธีการประเมิน
นำเสนอแผนงานละเอียดครบถ้วน ระบุ Timeline ชัดเจน และมีตัวอย่าง Playbook สำหรับ สขญ. ล่วงหน้า 5 รูปแบบขึ้นไป	100	ประเมินจากข้อมูลและเอกสารที่ผู้ให้บริการยื่นข้อเสนอมา โดยมีแผนงานและตัวอย่าง Playbook **ที่สอดคล้องกับบริบทของ สขญ.**
นำเสนอแผนงานละเอียดครบถ้วน และมีตัวอย่าง Playbook สำหรับ สขญ. 3-4 รูปแบบ	60	
นำเสนอแผนงานไม่ชัดเจน หรือมีตัวอย่าง Playbook น้อยกว่า 3 รูปแบบ	0	

10. สถานที่ติดต่อขอรับทราบข้อมูลเพิ่มเติม

สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)
234/432 ซอยลาดพร้าว 12 แขวงจอมพล
เขตจตุจักร กรุงเทพมหานคร 10900
ไปรษณีย์อิเล็กทรอนิกส์ susit.ta@bdi.or.th
website www.bdi.or.th

คณะกรรมการจัดทำขอบเขตของงาน

ลงชื่อ..... ประธานกรรมการ
(นายอนุรักษ์ ตันตราธิปไตย)

ลงชื่อ.....กรรมการ
(นายอภิณัฐ ก่ำบำรุง)

ลงชื่อ.....กรรมการและเลขานุการ
(นายสุศิษฐิ์ ต๊ะมามูล)

ภาคผนวก

เอกสาร ก1 ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น

1. ข้อมูลการประสานงาน

ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม

วันที่และเวลาที่แจ้ง

2. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม

3. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม

ชื่อ-นามสกุล ตำแหน่งงาน

ชื่อหน่วยงาน อีเมล

โทรศัพท์ (ที่ทำงาน / มือถือ)

4. ความต่อเนื่องของเหตุภัยคุกคาม

☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม

5. ลักษณะภัยคุกคามทางไซเบอร์

ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่

เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[1] ในระดับใด (มาตรา 60)

☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข)

☐ ยังไม่สามารถระบุได้

6. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า 1 รายการ)

หมวดหมู่*	คำอธิบาย
หมวดหมู่ที่ 2	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
หมวดหมู่ที่ 3	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
หมวดหมู่ที่ 4	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
หมวดหมู่ที่ 5	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
หมวดหมู่ที่ 6	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
หมวดหมู่ที่ 7	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
หมวดหมู่ที่ 8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ 0 หมวดหมู่ที่ 1 และหมวดหมู่ที่ 9 ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

[1] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ส่วนที่ 1

หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น

หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.): โปรดระบุ
หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี): โปรดระบุ
วันที่: เลือกวันที่ **เวลา:** โปรดระบุ

ก1. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม
ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ
ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ

ก2. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม
ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ
ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ
โทรศัพท์ (ที่ทำงาน / มือถือ) : โปรดระบุ

ก3. ความต่อเนื่องของเหตุภัยคุกคาม
☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม

ก4. ลักษณะภัยคุกคามทางไซเบอร์
ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน
☐ ใช่ ☐ ไม่ใช่
เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[2] ในระดับใด (มาตรา 60)
☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข)
☐ ยังไม่สามารถระบุได้

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์

ข1. วัน เวลา ที่เกิดเหตุภัยคุกคาม
วันที่ : เลือกวันที่ เวลา : โปรดระบุ
วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม
วันที่ : เลือกวันที่ เวลา : โปรดระบุ

ข2. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ
☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว _____

ข3. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า 1 รายการ)

หมวดหมู่*	คำอธิบาย
☐ หมวดหมู่ที่ 2	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
☐ หมวดหมู่ที่ 3	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน

[2] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำ หรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

	(Non-Compliance Activity)
☐ หมวดหมู่ที่ 4	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
☐ หมวดหมู่ที่ 5	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
☐ หมวดหมู่ที่ 6	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
☐ หมวดหมู่ที่ 7	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
☐ หมวดหมู่ที่ 8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
☐ อื่น ๆ	โปรดระบุ

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 (ทั้งนี้ ภัยคุกคามหมวดหมู่ที่ 0 1 และ 9 ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

ข4. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ:

สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง):

โปรดระบุ

ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ :

โปรดระบุ

บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการโอนเงิน):

โปรดระบุ

ฮาร์ดแวร์ ซอฟต์แวร์ที่ได้รับผลกระทบ (โปรดระบุรายละเอียด เช่น ผู้ผลิตหรือยี่ห้อ รุ่นของเครื่องคอมพิวเตอร์): โปรดระบุรายละเอียด

มีผลกระทบต่อการสื่อสาร (ทางโทรศัพท์ หรือ การใช้งานเครือข่าย): โปรดระบุ

รายละเอียดอื่น ๆ: โปรดระบุ

หมวด ค: ข้อมูลการรับมือภัยคุกคาม

ค1. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า 1 รายการ)

☐ เพิ่งพบเหตุการณ์ ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ

☐ อยู่ในขั้นตอนการสอบสวน ☐ กำลังลุกลาม

☐ อยู่ในขั้นตอนการระงับภัย ☐ สามารถระงับภัยได้แล้ว

☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว ☐ อื่น ๆ: โปรดระบุ

ค2. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว

☐ ยังไม่ได้ดำเนินการแก้ไขใด ๆ ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว

☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว

☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว

☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ

ค3. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี)

โปรดระบุ

ส่วนที่ 2

หมวด ง : รายละเอียดภัยคุกคาม

ง1. ข้อมูลการตรวจจับและการวิเคราะห์

ง1.1 <u>วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ</u> (System Access)

วันที่: เลือกวันที่ **เวลา:** โปรดระบุ **ไม่ทราบ:** ☐

ง1.2 ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์

รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม (เท่าที่ทราบ เช่น คน, ความผิดพลาดของระบบ, ภัยธรรมชาติ, การจู่โจม, ความผิดพลาดจากคนนอกองค์กร):

โปรดระบุ

บุคคล วิธี หรือเครื่องมือที่ตรวจพบภัยคุกคาม (เช่น ผู้ใช้, ผู้ดูแลระบบ, โปรแกรม Anti-virus, IDS, การวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์, ไม่ทราบ):

โปรดระบุ

รายละเอียดของปัญหาลักษณะคล้ายกันที่หน่วยงานเคยพบมาก่อน (ถ้ามี โปรดระบุรายละเอียด):

โปรดระบุ

ง1.3 รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล)

จำนวนระบบ บริการ หรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: โปรดระบุ

จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

มูลค่าความเสียหาย (โดยประมาณ): โปรดระบุ

ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย):

จำนวนบุคคลที่เป็นเจ้าของข้อมูล : โปรดระบุ

ชนิดของข้อมูล (เลือกทุกข้อที่ใช่):

☐ ข้อมูลไบโอเมตริกซ์ ☐ ข้อมูลการติดต่อ

☐ ข้อมูลการเงิน ☐ ข้อมูลบุคลากรของรัฐ

☐ หมายเลขบัตรประชาชน ☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ

☐ ข้อมูลทางการแพทย์

☐ อื่น ๆ : โปรดระบุ

จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ

ผลกระทบอื่น ๆ ที่เกิดขึ้น: โปรดระบุ

ง1.4 <u>รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)</u>

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้จู่โจม: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น: โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า 1 รายการ)

☐ ระบบล่ม ☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ

☐ บัญชีผู้ใช้ถูกสร้างขึ้นมาใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ

☐ การจู่โจมด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ

☐ ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)

☐ การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ

☐ การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ

☐ การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย

☐ การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง

☐ การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก

☐ การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย

☐ รูปแบบการใช้งานที่ผิดปกติ ☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ

☐ ความพยายามที่จะเขียนไฟล์ของระบบ ☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ

☐ การแก้ไขหรือลบข้อมูลที่ผิดปกติ ☐ การจู่โจมให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)

☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ ☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ผิดปกติ

☐ การแก้ไขหน้าเว็บ ☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น

☐ การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ

☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility)

☐ สิ่งที่ผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ

ง1.5 รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การจู่โจมครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการจู่โจม, Attack vector, เทคนิคหรือเครื่องมือที่ผู้จู่โจมใช้ ฯลฯ) โปรดระบุ

ง1.6 รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ

ง2. ข้อมูลการระงับ ปราบปราม และฟื้นฟู: โปรดระบุ

ง2.1 รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ

ง2.2 การคาดการณ์ความสามารถฟื้นฟู

โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

ง3. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)

ง3.1 วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ **เวลา:** โปรดระบุ
ง3.2 การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ
ง3.3 บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ

เอกสาร ก3 แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ 1 สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์[3]

หมวดหมู่	คำอธิบาย	จำนวน
0	เหตุการณ์จำลองและการฝึกจู่โจมของหน่วยงาน (Training and Exercises)	
1	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)	
2	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	
3	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)	
4	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)	
5	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	
6	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	
7	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	
8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)	
9	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)	

ข้อ 2 สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ

ทรัพย์สินที่ได้รับผลกระทบ	จำนวน
เครื่องแม่ข่าย / แอคทีฟ ไดเรกทอรี (Active Directory)	
เครื่องเวิร์กสเตชัน (Workstation)	
สวิตช์ (Switch) /เราเตอร์ (Router)	
เว็บไซต์ (Website)	
อื่น ๆ	

ข้อ 3 สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์[4]

ระดับภัยคุกคาม	จำนวน
ไม่ร้ายแรง	
ร้ายแรง	
วิกฤต (ก)	
วิกฤต (ข)	

[3] หมวดหมู่ตามข้อ 1 ของภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ.2564

[4] ระดับภัยคุกคามทางไซเบอร์ตามมาตรา 60 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562