แบบ บก.06

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย
การจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ โครงการจัดซื้อสิทธิการใช้งาน Software สำหรับพัฒนาระบบวิเคราะห์ ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหล
2. หน่วยงานเจ้าของโครงการ ศูนย์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (ธนาคารอาคารสงเคราะห์)
3. วงเงินงบประมาณที่ได้รับจัดสรร 12,000,000.00 บาท (สิบสองล้านบาทถ้วน) (รวมภาษีมูลค่าเพิ่มแล้ว)
4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ - 3 ก.พ. 2569
   เป็นเงิน (รวมภาษีมูลค่าเพิ่มแล้ว) 11,700,000.00 บาท (สิบเอ็ดล้านเจ็ดแสนบาทถ้วน)
   ราคา/หน่วย (ถ้ามี) .....บาท
5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
   พิจารณาตามข้อบังคับธนาคารอาคารสงเคราะห์ฉบับที่ 80 ว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุที่เกี่ยวกับการพาณิชย์โดยตรง พ.ศ.2561 ซึ่งสามารถจัดซื้อจัดจ้างได้จริงตามลำดับ ดังนี้
   (1) ราคาที่ได้มาจากการคำนวณตามหลักเกณฑ์ที่คณะกรรมการราคากลางกำหนด
   (2) ราคาที่ได้มาจากฐานข้อมูลราคาอ้างอิงของพัสดุที่กรมบัญชีกลางจัดทำ
   (3) ราคามาตรฐานที่สำนักงบประมาณหรือหน่วยงานกลางอื่นกำหนด
   (4) ราคาที่ได้มาจากการสืบราคาจากท้องตลาด
   (5) ราคาที่เคยซื้อหรือจ้างครั้งหลังสุดภายในระยะเวลาสองปีงบประมาณ
   (6) ราคาอื่นใดตามหลักเกณฑ์ วิธีการ หรือแนวทางปฏิบัติของธนาคาร
   ซึ่งเมื่อพิจารณาราคากลางตามข้อบังคับธนาคารอาคารสงเคราะห์ฉบับที่ 80 ตามลำดับแล้ว ไม่พบราคากลางตาม (1) (2) และ (3) จึงเห็นควรให้ใช้ราคากลางตามข้อ (4) โดยพิจารณาราคาต่ำสุด เป็นเงิน 11,700,000.00 บาท (สิบเอ็ดล้านเจ็ดแสนบาทถ้วน) (รวมภาษีมูลค่าเพิ่มแล้ว) ซึ่งได้สืบราคาจากท้องตลาดจำนวน 4 ราย ดังนี้
   5.1 บริษัท อินฟินิตี้ ทู อินฟินิตี้ จำกัด
   5.2 บริษัท ยิบอินซอย จำกัด
   5.3 บริษัท เอ็กซ์ฟินิท จำกัด
   5.4 บริษัท เซิร์ฟทริโอ อินโนเวชั่น จำกัด
6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นางศรีสุดา ยุทธเทพา	ประธานกรรมการ	
6.2 นายพัลลภ ม่วงไหมทอง	กรรมการ	
6.3 นายฉนานนท์ ตันสกุล	กรรมการ	
6.4 นายเอกณัฏฐ์ อเนกเจริญวณิช	กรรมการ	
6.5 นายณัฐวัฐ รุจิวรารัตน์	กรรมการ	
6.6 นายธีระชัย วิสุทธิพันธ์	กรรมการและเลขานุการ	

ขอบเขตงาน (Terms of Reference : TOR)
โครงการจัดซื้อสิทธิการใช้งาน Software สำหรับพัฒนาระบบวิเคราะห์
ติดตามภัยคุกคาม ทางไซเบอร์และตรวจจับข้อมูลรั่วไหล
เลขที่ 102-021/67

1. ความเป็นมา/เหตุผลและความจำเป็น

ความเจริญก้าวหน้าด้านเทคโนโลยีสารสนเทศและการสื่อสารเข้ามามีบทบาทมากขึ้น ในขณะเดียวกันพบว่าปัญหาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ความเสี่ยงจากภัยคุกคามทางด้านไซเบอร์ ที่เพิ่มมากขึ้น และมีแนวโน้มที่จะขยายตัวเพิ่มขึ้นในทุกภาคส่วน ซึ่งภัยคุกคามดังกล่าวอาจสามารถสร้างความเสียหายให้กับธนาคารได้อย่างมาก การเฝ้าระวัง และติดตามข่าวสารภัยคุกคาม ทางไซเบอร์ที่เกิดขึ้น รวมไปถึงการตรวจจับข้อมูลรั่วไหล จึงมีความสำคัญ ดังนั้นธนาคารจึงจำเป็นต้องจัดซื้อสิทธิการใช้งาน Software สำหรับพัฒนาระบบวิเคราะห์ ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหล เพื่อให้ธนาคารสามารถ หาแนวทางในการยับยั้ง เฝ้าระวัง รับมือ รวมไปถึงบริหารจัดการภัยคุกคามที่เกิดขึ้นกับระบบสารสนเทศของธนาคารได้

2. วัตถุประสงค์

เพื่อจัดซื้อสิทธิการใช้งาน Software สำหรับพัฒนาระบบวิเคราะห์ ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหล ที่สามารถทำงานร่วมกับระบบจัดเก็บบันทึกและวิเคราะห์เหตุการณ์ (Central Log Management System) ของธนาคาร สนับสนุนการทำงานทางด้านการตรวจสอบ สอบทาน วิเคราะห์ เฝ้าระวัง ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหล ซึ่งสนับสนุนวัตถุประสงค์เชิงยุทธศาสตร์ของธนาคาร (SO5 : ยกระดับการกำกับดูแลองค์กรเพื่อความยั่งยืน)

3. คุณสมบัติของผู้เสนอราคา

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบ ที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้าง และการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพตามที่จัดซื้อดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ธนาคาร ณ วันประกาศจัดซื้อ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการจัดซื้อครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอต้องไม่เคยถูกยกเลิกสัญญาซื้อขาย หรือสัญญาจ้างบริการบำรุงรักษาฯ ก่อนหมดอายุสัญญา โดยไม่มีเหตุผลอันควรจากธนาคาร หรือหน่วยงานใดๆ

3.11 ผู้ยื่นข้อเสนอทุกรายจะต้องเก็บรักษาข้อมูลที่เกี่ยวข้องทั้งหมดของธนาคารไว้เป็นความลับ จะไปเผยแพร่ที่อื่นมิได้

3.12 ผู้ยื่นข้อเสนอต้องทำความเข้าใจในเอกสารทุกฉบับให้เป็นที่เข้าใจโดยชัดแจ้ง และไม่ว่ากรณีใดๆผู้ยื่นข้อเสนอจะยกขึ้นเป็นข้ออ้างโดยอาศัยเหตุจากการที่ละเลย ไม่ทำความเข้าใจในข้อความดังกล่าว หรือละเลยไม่ปฏิบัติตามข้อความนั้น หรือโดยอ้างความสำคัญผิดในความหมายของข้อความในใบเสนอราคาเพื่อปฏิเสธความรับผิดชอบมิได้

3.13 หากธนาคารพบหรือทราบเมื่อใดก็ตามว่า ผู้ยื่นข้อเสนอมีเจตนาที่จะปิดบัง บิดเบือน หรือพยายามให้ธนาคารเข้าใจผิดไปจากความเป็นจริง ธนาคารจะพิจารณาตัดสิทธิในการเสนอราคา หรือยกเลิกสัญญา ที่ได้ทำไว้กับผู้ยื่นข้อเสนอ และเรียกค่าเสียหายที่พึงเกิดขึ้นจากการกระทำดังกล่าว

3.14 ยื่นข้อเสนอต้องยืนยันว่าพร้อมที่จะลงนามในสัญญาตามแบบสัญญาของธนาคาร รวมทั้งเงื่อนไขต่างๆ ในโครงการจัดซื้อสิทธิการใช้งาน Software สำหรับพัฒนาระบบวิเคราะห์ ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหล ของธนาคาร ข้อเสนอของผู้ยื่นข้อเสนอรวมทั้งข้อเสนอเพิ่มเติมในการต่อรองให้ถือเป็นส่วนหนึ่งของสัญญาด้วย

3.15 ผู้ยื่นข้อเสนอต้องเป็นบริษัทหรือห้างหุ้นส่วนนิติบุคคล ซึ่งเป็นผู้มีอาชีพดำเนินธุรกิจในด้านการจำหน่าย การจัดหา Software ที่ใช้เทคโนโลยี หรือต้องเป็นผู้แทนจำหน่าย Software หรือเคยมีผลงานการติดตั้ง Software ลักษณะเดียวกันกับโครงการนี้ ซึ่งมีหลักฐานยืนยันฐานะดังกล่าวนี้ต่อธนาคารได้

3.16 ผู้ยื่นข้อเสนอต้องมีบุคลากรในทีมงานที่จะเข้ามาดำเนินการติดตั้ง/ให้คำแนะนำ การใช้งาน Software สำหรับพัฒนาระบบวิเคราะห์ ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหล ที่ได้รับประกาศนียบัตร อย่างน้อย 3 คน ดังนี้

(1) ด้านการบริหารจัดการทีมเฝ้าระวังและตอบสนองต่อภัยคุกคามทางไซเบอร์ จำนวน 1 คน

- CompTIA Advanced Security Practitioner (CASP+) หรือ
- Certified Information Systems Security Professional (CISSP) หรือ
- Certified Information Security Management (CISM) หรือ
- CompTIA CySA+

(2) ด้านการเฝ้าระวังหรือตอบสนองต่อภัยคุกคามทางไซเบอร์ จำนวน 1 คน

- MITRE ATT&CK for Threat Hunting Detection Engineering หรือ
- eLearnSecurity Certified Incident Responder (eCIR) หรือ
- CompTIA CySA+ หรือ
- CompTIA Security+

(3) ด้านการทดสอบบุกรุกระบบ การวิจัย หรือการวิเคราะห์ภัยคุกคามทางไซเบอร์ จำนวน 1 คน

- MITRE ATT&CK for Cyber Threat Intelligence หรือ
- OSCP หรือ OSCP+ หรือ
- eLearnSecurity Certified Threat Hunting Professional (eCTHP) หรือ
- EC-Council C|EH หรือ
- CompTIA CySA+ หรือ
- CompTIA Pentest+

4. หลักฐานการเสนอราคา

ผู้ยื่นข้อเสนอจะต้องเสนอเอกสารหลักฐานยื่นมาพร้อมกับซองใบเสนอราคา โดยแยกไว้นอกซองใบเสนอราคาเป็น 2 ส่วน คือ

4.1 ส่วนที่ 1 อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(1) ในกรณีผู้เสนอราคาเป็นนิติบุคคล

(ก) ห้างหุ้นส่วนสามัญหรือห้างหุ้นส่วนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล บัญชีรายชื่อหุ้นส่วนผู้จัดการ ผู้มีอำนาจควบคุม พร้อมรับรองสำเนาถูกต้อง

(ข) บริษัทจำกัดหรือบริษัทมหาชนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล หนังสือบริคณห์สนธิบัญชีรายชื่อกรรมการผู้จัดการ ผู้มีอำนาจควบคุม และบัญชีผู้ถือหุ้นรายใหญ่ พร้อมรับรองสำเนาถูกต้อง

(2) ในกรณีผู้เสนอราคาเป็นบุคคลธรรมดาหรือคณะบุคคลที่มิใช่นิติบุคคล ให้ยื่นสำเนาบัตรประจำตัวประชาชนของผู้นั้น สำเนาข้อตกลงที่แสดงถึงการเข้าเป็นหุ้นส่วน (ถ้ามี) สำเนาบัตรประจำตัวประชาชนของผู้เป็นหุ้นส่วน พร้อมทั้งรับรองสำเนาถูกต้อง

(3) ในกรณีผู้เสนอราคาเป็นผู้เสนอราคาร่วมกันในฐานะเป็นผู้ร่วมค้า ให้ยื่นสำเนาสัญญา ของการเข้าร่วมค้า สำเนาบัตรประจำตัวประชาชนของผู้ร่วมค้า และในกรณีที่ผู้เข้าร่วมค้าฝ่ายใดเป็นบุคคลธรรมดาที่มิใช่สัญชาติไทย ก็ให้ยื่นสำเนาหนังสือเดินทาง หรือผู้ร่วมค้าฝ่ายใด เป็นนิติบุคคลให้ยื่นเอกสารตามที่ระบุไว้ใน (1)

(4) บัญชีเอกสารส่วนที่ 1 ทั้งหมดที่ได้ยื่นพร้อมกับซองใบเสนอราคา

4.2 ส่วนที่ 2 อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(1) แค็ตตาล็อกหรือแบบรูปรายละเอียดคุณลักษณะเฉพาะ

(2) ตารางเปรียบเทียบคุณลักษณะเฉพาะของ Software สำหรับพัฒนาวิเคราะห์ ติดตามภัยคุกคามทางไซเบอร์ และตรวจจับข้อมูลรั่วไหล ที่เสนอกับคุณลักษณะเฉพาะที่ธนาคารกำหนด

(3) หนังสือมอบอำนาจซึ่งปิดอากรแสตมป์ตามกฎหมายในกรณีที่ผู้ยื่นข้อเสนอราคามอบอำนาจให้บุคคลอื่นลงนามในใบเสนอราคาแทน

(4) บัญชีเอกสารส่วนที่ 2 ทั้งหมดที่ได้ยื่นพร้อมกับซองใบเสนอราคา

5. เอกสารประกอบการเสนอราคา

5.1 ข้อมูลเกี่ยวกับประวัติ และความเป็นมาของบริษัทผู้ยื่นข้อเสนอ รวมถึงลักษณะการดำเนินงานผลประกอบการที่ผ่านมา รายชื่อลูกค้าสำคัญ ภายในประเทศ และ/หรือ ภายนอกประเทศที่อ้างอิงได้

5.2 ผู้ยื่นข้อเสนอต้องทำความเข้าใจในเอกสารทุกฉบับให้เป็นที่เข้าใจโดยชัดแจ้ง และไม่ว่ากรณีใด ๆ ผู้ยื่นข้อเสนอจะยกขึ้นเป็นข้ออ้างโดยอาศัยเหตุจากการที่ละเลย ไม่ทำความเข้าใจในข้อความดังกล่าว หรือละเลยไม่ปฏิบัติตามข้อความนั้น หรือโดยอ้างความสำคัญผิดในความหมาย ของข้อความในใบเสนอราคาเพื่อปฏิเสธความรับผิดชอบมิได้

5.3 หากธนาคารพบหรือทราบเมื่อใดก็ตามว่า ผู้ยื่นข้อเสนอมีเจตนาที่จะปิดบัง บิดเบือน หรือพยายามให้ธนาคารเข้าใจผิดไปจากความเป็นจริง ธนาคารจะพิจารณาตัดสิทธิในการเสนอราคา หรือ ยกเลิกสัญญา ที่ได้ทำไว้กับผู้ยื่นข้อเสนอ และเรียกค่าเสียหายที่พึงเกิดขึ้นจากการกระทำดังกล่าว

5.4 ผู้ยื่นข้อเสนอต้องยืนยันว่าพร้อมที่จะลงนามในสัญญาตามแบบสัญญาของธนาคาร รวมทั้งเงื่อนไขต่างๆ ในการจัดซื้อ Software สำหรับพัฒนาระบบวิเคราะห์ ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหล ของธนาคาร ข้อเสนอของผู้ยื่นข้อเสนอรวมทั้งข้อเสนอเพิ่มเติมในการต่อรองให้ถือเป็นส่วนหนึ่ง ของสัญญาด้วย

5.5 รายละเอียดต่างๆ ที่ผู้ยื่นข้อเสนอเสนอมานั้น หากมีปัญหาในการตีความของข้อความใด ให้ถือคำวินิจฉัยของธนาคารเป็นที่ยุติ

6. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

การพิจารณาผู้ชนะการยื่นข้อเสนอ ธนาคารจะพิจารณาจากเกณฑ์ราคา

7. การทำสัญญา

ผู้ได้รับการคัดเลือกจะต้องติดต่อธนาคารเพื่อทำสัญญาภายใน 7 วัน นับถัดจากวันที่ได้รับแจ้ง เป็นหนังสือ และจะต้องวางหลักประกันสัญญาเป็นจำนวนเงินเท่ากับร้อยละ 5 ของมูลค่าสัญญาและให้ธนาคารยึดถือไว้ในขณะทำสัญญา โดยใช้หลักประกันอย่างหนึ่งอย่างใด ดังต่อไปนี้

7.1 เงินสด

7.2 เช็คหรือดราฟท์ที่ธนาคารเซ็นสั่งจ่าย ซึ่งเป็นเช็คหรือดราฟท์ลงวันที่ที่ใช้เช็คหรือดราฟท์นั้นชำระต่อเจ้าหน้าที่ หรือก่อนหน้านั้นไม่เกิน 3 วัน ทำการ

7.3 หนังสือค้ำประกันของธนาคารภายในประเทศตามตัวอย่างที่คณะกรรมการนโยบายกำหนด โดยอาจเป็นหนังสือค้ำประกันอิเล็กทรอนิกส์ตามวิธีการที่กรมบัญชีกลางกำหนดก็ได้

7.4 หนังสือค้ำประกันของบรรษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยอนุโลมให้ใช้ตามตัวอย่างหนังสือค้ำประกันของธนาคารที่คณะกรรมการนโยบายกำหนด

7.5 พันธบัตรรัฐบาลไทย

หลักประกันนี้จะคืนให้โดยไม่มีดอกเบี้ย ภายใน 15 วัน นับถัดจากวันที่คู่สัญญาพ้นจากข้อผูกพันตามสัญญาแล้ว

ทั้งนี้ หากผู้ได้รับการคัดเลือกไม่ดำเนินการภายในระยะเวลาดังกล่าวข้างต้น ธนาคารสงวนสิทธิ์ที่จะยกเลิกการจัดซื้อ และพิจารณาแจ้งเป็นผู้ทิ้งงาน

8. รายละเอียดของงานที่จะจัดซื้อ

ผู้ยื่นข้อเสนอต้องนำเสนอ Software สำหรับพัฒนาระบบวิเคราะห์ ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหล พร้อมติดตั้ง โดยมีรายละเอียดของงาน ตามเอกสารแนบ

9. ระยะเวลาดำเนินการ

ระยะเวลาดำเนินการส่งมอบสิทธิการใช้งาน พร้อมติดตั้ง Software สำหรับพัฒนาระบบวิเคราะห์ ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหล ภายใน 60 วัน นับถัดจากวันที่ลงนามในสัญญา โดยมีเงื่อนไขตามเอกสารแนบ

10. วงเงินที่จะจัดซื้อ

วงเงินงบประมาณ 12,000,000.- บาท (สิบสองล้านบาทถ้วน)

11. เงื่อนไขการชำระเงิน

ธนาคารจะชำระเงินค่าจัดซื้อสิทธิการใช้งาน Software สำหรับพัฒนาระบบวิเคราะห์ ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหล หลังจากที่ได้ตรวจรับการส่งมอบงานถูกต้องครบถ้วนเรียบร้อยตามเงื่อนไขสัญญา ตามที่ธนาคารกำหนด โดยจะชำระเงิน แบ่งเป็น 2 งวด ตามเงื่อนไข ดังนี้

งวดที่ 1 จำนวน 30% ของมูลค่าตามสัญญา (ภายในระยะเวลา 30 วัน นับถัดจากวันลงนามในสัญญา) เมื่อผู้ได้รับการคัดเลือกดำเนินการจัดส่งสิทธิการใช้งาน Software สำหรับพัฒนาระบบวิเคราะห์ ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหลเรียบร้อยแล้ว

งวดที่ 2 จำนวน 70% ของมูลค่าตามสัญญา (ภายในระยะเวลา 60 วัน นับถัดจากวันลงนามในสัญญา) เมื่อผู้ได้รับการคัดเลือกดำเนินการติดตั้ง Software สำหรับพัฒนาระบบวิเคราะห์ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหล รวมถึงดำเนินการฝึกอบรม และคณะกรรมการตรวจรับได้ตรวจรับมอบแล้วเห็นว่าถูกต้อง ตรงตามเงื่อนไขของสัญญา

12. อัตราค่าปรับ

กำหนดค่าปรับเป็นรายวันในอัตราร้อยละ 0.20 ของราคาพัสดุที่ยังไม่ได้รับมอบ

13. ระยะเวลาการใช้งาน/สิทธิการใช้งาน

ผู้ได้รับการคัดเลือกต้องรับประกันให้ธนาคารสามารถใช้ Software สำหรับพัฒนาระบบวิเคราะห์ ติดตามภัยคุกคาม ทางไซเบอร์และตรวจจับข้อมูลรั่วไหล ได้เป็นอย่างดีเป็นระยะเวลา 1 ปี นับถัดจากวันที่ธนาคารได้ตรวจรับมอบโดยถูกต้องครบถ้วนตามสัญญา โดยไม่คิดค่าใช้จ่ายใดๆ ทั้งสิ้น ในระหว่างระยะเวลาการรับประกันดังกล่าว

14. ข้อสงวนสิทธิ์ในการยื่นข้อเสนอและอื่นๆ

14.1 ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกยินยอมให้ธนาคารอาคารสงเคราะห์ ธนาคารแห่งประเทศไทย และ/หรือหน่วยงานอื่นที่กำกับดูแลธนาคารอาคารสงเคราะห์ตามกฎหมาย รวมทั้ง ผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก ที่ได้รับการแต่งตั้งจากธนาคารแห่งประเทศไทย ธนาคารอาคารสงเคราะห์ หรือหน่วยงานอื่นที่กำกับดูแลธนาคารอาคารสงเคราะห์ตามกฎหมาย มีสิทธิเข้าตรวจสอบการดำเนินงาน และ/หรือการควบคุมภายในของผู้ยื่นข้อเสนอที่ได้รับการคัดเลือก และ/หรือบุคคลภายนอกที่เกี่ยวข้องกับผลิตภัณฑ์

14.2 ธนาคารสงวนสิทธิ์ที่จะแก้ไขเพิ่มเติมเงื่อนไข หรือข้อกำหนดในแบบสัญญาหรือข้อตกลงซื้อเป็นหนังสือ ให้เป็นไปตามความเห็นของสำนักงานอัยการสูงสุด (ถ้ามี)

14.3 ในกรณีที่เอกสารแนบท้ายเอกสารการจัดซื้อ มีความขัดหรือแย้งกัน ผู้ยื่นข้อเสนอจะต้องปฏิบัติตามคำวินิจฉัยของธนาคาร คำวินิจฉัยดังกล่าวให้ถือเป็นที่สุด และผู้ยื่นข้อเสนอ ไม่มีสิทธิเรียกร้องค่าใช้จ่ายใด ๆ เพิ่มเติม

14.4 ธนาคารอาจประกาศยกเลิกการจัดซื้อในกรณีต่อไปนี้ได้ โดยที่ผู้ยื่นข้อเสนอจะเรียกร้อง ค่าเสียหาย ใด ๆ จากธนาคารไม่ได้

(1) ธนาคารไม่ได้รับการจัดสรรเงินที่จะใช้ในการจัดซื้อหรือที่ได้รับจัดสรรแต่ไม่เพียงพอ ที่จะทำการจัดซื้อครั้งนี้ต่อไป

(2) มีการกระทำที่เข้าลักษณะผู้ยื่นข้อเสนอที่ชนะการจัดซื้อหรือที่ได้รับการคัดเลือกมีผลประโยชน์ร่วมกัน หรือมีส่วนได้เสียกับผู้ยื่นข้อเสนอรายอื่น หรือขัดขวางการแข่งขัน อย่างเป็นธรรม หรือสมยอมกันกับผู้ยื่นข้อเสนอรายอื่น หรือเจ้าหน้าที่ในการเสนอราคา หรือส่อว่ากระทำการทุจริตอื่นใดในการเสนอราคา

(3) การทำการจัดซื้อครั้งนี้ต่อไปอาจก่อให้เกิดความเสียหายแก่ธนาคาร หรือกระทบต่อประโยชน์สาธารณะ

(4) กรณีอื่นในทำนองเดียวกับ (1) (2) หรือ (3) ตามที่กำหนดในกฎกระทรวง ซึ่งออกตาม ความในกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ

15. การปฏิบัติตามกฎหมายและระเบียบ

ในระหว่างระยะเวลาการซื้อ ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ขายต้องปฏิบัติ ตามหลักเกณฑ์ ที่กฎหมายและระเบียบได้กำหนดไว้โดยเคร่งครัด

16. หน่วยงานที่รับผิดชอบ

ศูนย์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โทร. 02-202-6659

ลงชื่อ.....ประธานกรรมการ
(นางศรีสุดา ยุทธเทพา)
ผู้อำนวยการศูนย์ความมั่นคงปลอดภัย
ด้านเทคโนโลยีสารสนเทศ

ลงชื่อ.....กรรมการ
(นายพัลลภ ม่วงไหมทอง)
หัวหน้าส่วนดูแลมาตรฐานความมั่นคงปลอดภัย
กฎข้อบังคับและประเมินความเสี่ยงระบบสารสนเทศ

ลงชื่อ.....กรรมการ
(นายฉนานนท์ ตันสกุล)
ผู้ช่วยหัวหน้าส่วน
ส่วนจัดการระบบเครือข่ายและความมั่นคงฯ

ลงชื่อ.....กรรมการ
(นายเอกณัฏฐ์ อเนกเจริญวณิช)
ผู้ช่วยหัวหน้าส่วน
ส่วนดูแลมาตรฐานความมั่นคงปลอดภัยฯ

ลงชื่อ.....กรรมการ
(นายณัฐรัฐ รุจิวรารัตน์)
พนักงานด้านความมั่นคงปลอดภัยเทคโนโลยี
สารสนเทศอาวุโส

ลงชื่อ.....กรรมการและเลขานุการ
(นายธีระชัย วิสุทธิพันธ์)
ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยเทคโนโลยี
สารสนเทศ

เอกสารแนบ

รายละเอียดและคุณลักษณะเฉพาะของโครงการจัดซื้อสิทธิการใช้งาน Software สำหรับพัฒนาระบบวิเคราะห์ ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหล

---

1. คุณลักษณะเฉพาะของพัสดุ

โครงการจัดซื้อสิทธิการใช้งาน Software สำหรับพัฒนาระบบวิเคราะห์ ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหล (เป็นระยะเวลา 1 ปี) ที่ธนาคารต้องการจัดหาเพื่อติดตั้งใช้งานที่ธนาคารอาคารสงเคราะห์ สำนักงานใหญ่ ประกอบด้วยส่วนหลัก 4 ส่วน ดังนี้

1.1 **Software ที่เสนอต้องทำงานร่วมกับระบบจัดเก็บบันทึกเหตุการณ์ (Central Log Management System) ที่เป็นผลิตภัณฑ์ Splunk ของธนาคาร และมีรายละเอียดย่อย ดังนี้**

1.1.1 สามารถทำงานร่วมกับ ระบบจัดเก็บบันทึกเหตุการณ์ของธนาคารได้ โดยการใช้ API

1.1.2 สามารถใช้ ระบบจัดเก็บบันทึกเหตุการณ์ของธนาคาร ในการสร้าง Dashboard เพื่อดึงข้อมูลจาก Software ที่เสนอมาแสดงได้

1.1.3 ต้องมี Application หรือ Add-on ที่สามารถทำงานและติดตั้งในระบบจัดเก็บบันทึกเหตุการณ์ (Splunk Dashboard) ของธนาคารได้

1.1.4 ผู้ได้รับการคัดเลือก ต้องสามารถดำเนินการร่วมกับทีมงานของธนาคาร/ผู้ให้บริการภายนอก ที่ธนาคารกำหนด ในการปรับตั้งค่า Software ที่เสนอ ให้สามารถทำงานร่วมกับ ระบบจัดเก็บบันทึกเหตุการณ์ ของธนาคารได้

1.1.5 ผู้ได้รับการคัดเลือก ต้องดำเนินการปรับตั้งค่า Configuration ของ Software ที่เสนอให้สามารถทำงานร่วมกับระบบจัดเก็บบันทึกเหตุการณ์ของธนาคารได้อย่างเต็มประสิทธิภาพ

1.2 **Software ที่เสนอจะต้องมีความสามารถติดตามข้อมูลข่าวสารภัยคุกคามไซเบอร์ (Threat Intelligence) และมีรายละเอียดย่อย ดังนี้**

1.2.1 ต้องเป็น Software ที่ออกแบบเพื่อรวบรวมข้อมูลภัยคุกคามไซเบอร์โดยเฉพาะ (Threat Intelligence)

1.2.2 สามารถใช้งานผ่าน Web Browser ได้เป็นอย่างน้อย

1.2.3 ธนาคารมีสิทธิ์การเข้าใช้งานพร้อมกันได้ไม่น้อยกว่า 5 ผู้ใช้งาน (Concurrent Users)

1.2.4 ต้องมีข้อมูลที่รวบรวมจากแหล่งต่าง ๆ มากกว่า 5 ปี ได้แก่ Open Source, Paste Site, Public Sources, Technical Sources, Deep/Dark Web, Underground Forum, Special Access Sites, Code Repositories เป็นอย่างน้อย รวมทั้งมีทีมนักวิจัยสำหรับวิเคราะห์ข้อมูลต่างๆ และ ยังรวบรวมจากแหล่งที่ไม่ใช่ภาษาอังกฤษด้วย และข้อมูลต้องถูกแปลความในรูปแบบภาษาไทย หรือ อังกฤษ

1.2.5 ต้องมีการให้ค่าตัวบ่งชี้ของการบุกรุก (IOC) พร้อมคะแนนความเชื่อถือคุณภาพของการตรวจจับหรือคะแนนความเสี่ยง (Risk score) โดยคะแนนที่แสดงจะต้องมีเอกสารอ้างอิงเกณฑ์การให้คะแนนหลังจากที่แสดงผลของคะแนนที่กำหนดไว้ และคะแนนต้องเป็นไปตามการเปลี่ยนแปลงปัจจุบัน (Dynamic) เพื่อแสดงความเสี่ยงแบบเรียลไทม์ที่เกิดขึ้นโดยอัตโนมัติสำหรับตัวบ่งชี้ของการบุกรุก (IOC) ที่กำลังตรวจสอบ

1.2.6 สามารถค้นหาข้อมูลภัยคุกคามไซเบอร์ อย่างน้อยดังนี้

1) Keyword หรือ IOCs เช่น IP Address, URL, Vulnerability, Domain, Hash, Malware, Threat Actor, Hashtag, Product เป็นต้น
2) ข้อมูลการโจมตีทางไซเบอร์ เช่น Malware, MITRE ATT&CK Identifier, Vulnerability และ Threat Actor เป็นต้น
3) Event Type เช่น Cyber Exploit, Cyber Attack, Vulnerability, Service Disruption, Infrastructure Analysis, และ Credential Leak เป็นต้น
4) Source Type เช่น App Store, Dark Web Data Dumps, Dark Web Market, Dark Web Ransomware Extortion Website, Paste Site, Security Breach Disclosures เป็นต้น

1.2.7 สามารถเฝ้าระวัง Traffic ที่ต้องสงสัย (C2 Communication) ระหว่างภัยคุกคาม (Threat/Attacker) และองค์กรเป้าหมาย (Victim) ได้ โดยที่ไม่จำเป็นต้องติดตั้ง Endpoint Agents ใด ๆ การวิเคราะห์การเชื่อมต่อเครือข่าย ที่เป็นอันตรายนี้

1.2.8 สามารถแสดงข้อมูลภัยคุกคามไซเบอร์ ซึ่งประกอบด้วยรายละเอียดอย่างน้อยดังนี้

1) ข้อมูลรายละเอียดปัจจัยแวดล้อมต่าง ๆ ที่เกี่ยวกับกลุ่มอาชญากรทางไซเบอร์ รวมถึงวิธีการป้องกันภัยคุกคามเหล่านั้น เช่น ข้อมูลกลุ่มอาชญากรทางไซเบอร์ (Threat Actor), วิธีการ โจมตี (Attack Vector), ช่องโหว่ที่ใช้โจมตี (Vulnerability), เป้าหมายที่ถูกโจมตี (Target) เป็นต้น ในรูปแบบ Tactics, Techniques, and Procedures (TTPs)
2) ข้อมูลช่องโหว่ (Vulnerability) ตามหมายเลข CVE, ระดับความรุนแรง (Severity), คะแนนความเสี่ยง (Risk Score), Product ที่ได้รับผลกระทบ และ NVD (National Vulnerability Database) Summary เป็นต้น
3) ข้อมูลตัวบ่งชี้ภัยคุกคาม (Indicators of Compromise – IOCs) ของภัยคุกคามนั้น ๆ ได้แก่ Domain name, IP Address, Vulnerability, Hash เป็นอย่างน้อย และมีคะแนนความเสี่ยง (Risk Score) แบบ Dynamics เพื่อช่วยในการตรวจสอบข้อมูล โดยมีการอ้างอิงแหล่งที่มาของแหล่งข้อมูลได้
4) ข้อมูลรายงาน (Exclusive Summary) ที่เกี่ยวข้องกับกลุ่มผู้โจมตี เช่น ข้อมูลสมาชิกและประวัติการรวมกลุ่มผู้โจมตี หรือ Malware

5) ข้อมูล Hunting Tool หรือ Hunting Package ได้แก่ Yara rules, Sigma rules และ MITRE ATT&CK เพื่อช่วยในการค้นหาข้อมูลภัยคุกคามที่ต้องการได้

6) ข้อมูล Intelligence Report จากการวิจัยภัยคุกคามจากเจ้าของผลิตภัณฑ์ (In-House Threat Researchers)

1.2.9 ข้อมูลภัยคุกคามไซเบอร์ที่แสดงผลจากการค้นหา ต้องมีการอ้างอิงถึงแหล่งที่มาของข้อมูล

1.2.10 สามารถแสดง Threat Actor Heat Map ที่เกี่ยวข้องได้

1.2.11 สามารถตรวจสอบ File หรือ URL ที่ต้องสงสัย โดย Upload File เพื่อทำการตรวจสอบด้วย วิธี Static Analysis และ Sandbox Analysis ด้วย Windows7, Windows10, macOS, Android และ Linux ได้

1.2.12 มี AI ที่ใช้ GPT (Generative Pre-trained Transformer) เพื่อให้ข้อมูลสรุปและการวิเคราะห์ภัยคุกคามต่างๆแบบ Real-time

1.2.13 ต้องใช้การเรียนรู้ Machine Learning และ Natural Language Processing (NLP) เพื่อเก็บรวบรวมและจัดโครงสร้างเนื้อหาของข้อความและข้อมูล จากแหล่งที่มาต่าง ๆ ในภาษาต่าง ๆ และจัดสามารถจัดเรียงหมวดหมู่ได้ จากแหล่งข้อมูลที่มาจากหลายภาษา

1.2.14 สามารถสร้าง Incident แจ้งเตือน ในกรณีที่เกิดเหตุการณ์ผิดปกติหรือเกิดความเสี่ยงได้ โดยอัตโนมัติและแจ้งเตือนผ่าน Email, Mobile App, Portal ไปยังผู้ดูแลระบบได้

1.3 **Software ที่เสนอจะต้องมีความสามารถในการติดตามข่าวสารเกี่ยวกับภัยคุกคามภายนอกที่ส่งผลต่อภาพลักษณ์องค์กร (Brand Intelligence) และมีรายละเอียดย่อย ดังนี้**

1.3.1 เป็น Software ที่ออกแบบเพื่อรวบรวมข้อมูลข่าวสารเกี่ยวกับภัยคุกคามภายนอกที่ส่งผลต่อภาพลักษณ์องค์กร โดยเฉพาะ (Brand Intelligence)

1.3.2 สามารถใช้งานผ่าน Web Browser ได้เป็นอย่างน้อย

1.3.3 สามารถตรวจจับข้อมูลรั่วไหล (Credential leak) โดยแจ้งเตือน (Alert) ให้ทราบได้

1.3.4 สามารถตรวจสอบเหตุข้อมูลรั่วไหล (Data or Credential Leak) เช่น รหัสผ่านที่รั่วไหลหรือถูกละเมิดจากอีเมลหรือโดเมนเนม

1.3.5 สามารถแสดง Screenshot ของ Phishing Domain ที่เกี่ยวข้อง รวมทั้งแสดง DNS Record และ Whois Record ได้

1.3.6 สามารถตรวจสอบสาเหตุข้อมูลรั่วไหลได้ ผ่าน GUI หรือ API โดยมี API Document อธิบายวิธีการใช้งานอย่างชัดเจน

1.3.7 ธนาคารมีสิทธิ์การเข้าใช้งานพร้อมกันได้ไม่น้อยกว่า 5 ผู้ใช้งาน (Concurrent Users)

1.3.8 มีข้อมูลที่รวบรวมจากแหล่งต่าง ๆ มากกว่า 5 ปี ได้แก่ Open Source, Paste Site, Deep/Dark Web, Underground forum เป็นอย่างน้อย

1.3.9 สามารถแจ้งเตือนเมื่อมีเหตุข้อมูลรั่วไหลเกิดขึ้นและเกี่ยวข้องกับอีเมลหรือโดเมนเนมของธนาคาร ที่กำหนด

1.3.10 สามารถแสดงข้อมูลเหตุรั่วไหล ที่ประกอบด้วย อีเมลหรือรหัสผ่านที่รั่วไหล และแหล่งข้อมูลอ้างอิง

1.3.11 สามารถค้นหา keyword จากการตรวจจับข้อความในภาพ (OCR) ได้

1.3.12 สามารถทำการ Monitor เช่น IP Address, Domain หรือ Brand Names Target List ได้ไม่น้อยกว่า 1,000 รายการ โดยแสดงแบบ Dashboard view ได้ เป็นอย่างน้อย

1.3.13 ในกรณีที่ตรวจพบภัยคุกคามที่ส่งผลต่อภาพลักษณ์องค์กร ผู้ได้รับคัดเลือกต้องดำเนินการ Takedown ตามกระบวนการทางกฎหมาย เมื่อได้รับแจ้งยืนยันจากธนาคาร จำนวนอย่างน้อย 20 Credits หรืออย่างน้อย 5 ครั้ง

1.4 **Software ที่เสนอจะต้องมีความสามารถในการตรวจสอบภัยคุกคามทางไซเบอร์ และแสดงผลข้อมูลบัญชีที่ถูกละเมิด (Identity Intelligence) และมีรายละเอียดย่อย ดังนี้**

1.4.1 ธนาคารมีสิทธิ์การเข้าใช้งานพร้อมกันได้ไม่น้อยกว่า 15 ผู้ใช้งาน (Concurrent Users)

1.4.2 เป็น Software ที่ออกแบบเพื่อแสดงข้อมูลบัญชีที่ถูกละเมิด (Account Takeover) โดยเฉพาะ เช่น Username, Password (Identity), Hostname, Malware Name, File Path Location ที่เกี่ยวข้องกับสาเหตุของข้อมูลที่รั่วไหลได้

1.4.3 สามารถแสดงข้อมูลที่เกี่ยวข้องกับบัญชีที่ถูกละเมิดได้ เช่น SHA1, MD5, SHA256, NTLM เป็นต้น ตามประเภทของข้อมูลที่รั่วไหล

1.4.4 สามารถปกปิดข้อมูล Password ที่รั่วไหล ที่อยู่ในรูปแบบ Plaintext ได้ โดยแสดงแค่บางตำแหน่งของรหัสผ่าน (Password) ทั้งนี้จะต้องสามารถส่งคำขอเพื่อแสดงรหัสผ่านทั้งหมดได้แบบ Clear text password

1.4.5 สามารถตั้งกรองค่าสำหรับการค้นหารหัสผ่านที่รั่วไหลบน internet ได้ แบบเฉพาะเจาะจง เช่น Uppercase/Lowercase Letter, Number, Symbol, Mixed Case, At least 8/12/16/24 characters

1.4.6 สามารถแสดงวันที่โดนขโมยข้อมูลรหัสผ่านของบัญชีที่ถูกละเมิดได้

1.4.7 สามารถแสดงให้เห็นถึงบริการของผู้ใช้ที่ถูกละเมิด ที่กำลังใช้งานอยู่ในกรณีของแอปพลิเคชั่นที่โฮสต์บนโดเมนนั้นๆ ได้

2. เงื่อนไขการติดตั้งและส่งมอบ

2.1 ผู้ที่ได้รับการคัดเลือกต้องจัดส่งสิทธิการใช้งาน Software สำหรับพัฒนาระบบวิเคราะห์ ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหล ที่ซื้อขาย ณ ธนาคารอาคารสงเคราะห์ สำนักงานใหญ่ ให้ครบถ้วนภายใน 30 วัน นับถัดจากวันที่ลงนามในสัญญา

2.2 ผู้ที่ได้รับการคัดเลือกจะต้องดำเนินการติดตั้ง Software สำหรับพัฒนาระบบวิเคราะห์ ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหล ที่ซื้อขาย ณ ธนาคารอาคารสงเคราะห์ สำนักงานใหญ่ ให้ครบถ้วนภายใน 60 วัน นับถัดจากวันที่ลงนามในสัญญา

2.3 ผู้ที่ได้รับการคัดเลือกจะต้องจัดส่งเอกสาร คู่มือฉบับภาษาไทย หรือ Media คู่มือการปฏิบัติงานของ Software สำหรับพัฒนาระบบวิเคราะห์ ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหล โดยต้องถูกรวบรวม และส่งมอบ ในลักษณะของแฟ้มงานจำนวน 1 แฟ้ม และจัดทำ Index ของเอกสาร แบ่งแยกเอกสารอย่างชัดเจนให้แก่ธนาคาร

2.4 ผู้ที่ได้รับการคัดเลือกจะต้องจัดให้มีเจ้าหน้าที่ที่มีความเชี่ยวชาญด้านเฝ้าระวังและตอบสนองต่อภัยคุกคามทางไซเบอร์ อย่างน้อย 1 ท่านเพื่อสนับสนุน ให้คำแนะนำ ในลักษณะ On The Job Training เกี่ยวกับ Software ที่เสนอหรือวิเคราะห์ภัยคุกคามที่เกิดขึ้น ตั้งแต่เวลา 08.30 – 16.30 น. (วันทำการ) (เป็นเวลารวมทั้งหมด 24 วัน) ภายในระยะเวลา 1 ปี (นับถัดจากวันที่ลงนามในสัญญา) โดยธนาคารจะเป็นผู้กำหนดวันเข้ามาปฏิบัติงานที่ธนาคาร เพื่อให้คำปรึกษาและดำเนินการปรับแต่งเพิ่มเติมและแก้ไขค่าคอนฟิก ของ Software หรือ อุปกรณ์ที่เกี่ยวข้องเพื่อให้สามารถทำงานได้อย่างมีประสิทธิภาพ

2.5 ผู้ที่ได้รับการคัดเลือกจะต้องจัดหลักสูตรการฝึกอบรมให้แก่ผู้ดูแลระบบ หัวข้อ การวิเคราะห์ ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหล ให้ครบถ้วนภายใน 60 วัน นับถัดจากวันที่ลงนามในสัญญา

2.6 ผู้ที่ได้รับการคัดเลือกจะต้องจัดหาสิทธิ์การเข้าใช้งาน Platform ทางด้าน Cyber Security (Blue Team) ที่มี Lab ให้ลงมือทำเชิงปฏิบัติได้จริง ให้เป็นกรรมสิทธิ์ของธนาคารเข้าใช้งานเป็นระยะเวลา 1 ปี แบบ Professional จำนวน 6 บัญชีผู้ใช้งาน โดย Platform ดังกล่าวต้องมี Lab ที่ครอบคลุม ให้แก่ Incident Response, Digital Forensics, Security Operations, Reverse Engineering และ Threat Intelligence ภายใน 60 วัน นับถัดจากวันที่ลงนามในสัญญา

2.7 ผู้ที่ได้รับการคัดเลือกต้องให้คำปรึกษา จัดทำ และปรับแต่งการทำงานของ Software ที่เสนอร่วมกับเจ้าหน้าที่ของธนาคาร เพื่อให้ Software ที่เสนอสามารถแจ้งเตือนเหตุการณ์ และจัดทำรายงาน/Dashboard ตามความต้องการของธนาคาร โดยแบ่งเป็น

2.6.1 รายงาน/Dashboard ตาม Template มาตรฐาน ที่มาพร้อมกับ Software สำหรับพัฒนาระบบวิเคราะห์ ติดตามภัยคุกคาม ทางไซเบอร์และตรวจจับข้อมูลรั่วไหล

2.6.2 รายงาน/Dashboard ข้อมูลรั่วไหลประจำวันที่เกี่ยวข้องตาม Asset List ของธนาคาร

2.6.3 รายงาน/Dashboard สรุปข้อมูลระบบสารสนเทศของธนาคาร ถูกโจมตีประจำวัน โดยอ้างอิงข้อมูลจาก Software ที่เสนอ

2.6.4 รายงาน/Dashboard แนวโน้มการเกิดภัยคุกคามกับระบบงานของธนาคาร โดยอ้างอิงข้อมูลจาก Software ที่เสนอ

3. การฝึกอบรม

ผู้ที่ได้รับการคัดเลือกต้องจัดการฝึกอบรมให้แก่ผู้เข้าฝึกอบรมของธนาคารภายในเวลา 60 วัน (นับถัดจากวันลงนามในสัญญา) ซึ่งมีหัวข้อของหลักสูตรที่ครอบคลุมทั้งภาคทฤษฎีและภาคปฏิบัติอย่างน้อย ดังนี้

ที่	ชื่อหลักสูตร	จำนวนวัน	สถานที่อบรม	จำนวนครั้ง	จำนวนคนต่อครั้ง
1	การวิเคราะห์ ติดตามภัยคุกคามทางไซเบอร์และตรวจจับข้อมูลรั่วไหล	2	ธนาคารอาคารสงเคราะห์ (สำนักงานใหญ่) หรือสถานที่ภายนอกที่ธนาคารกำหนด	1	6

ทั้งนี้ การฝึกอบรมทุกครั้ง ผู้ที่ได้รับการคัดเลือกจะต้องเป็นผู้ดำเนินการจัดหาติดตั้งอุปกรณ์ที่เกี่ยวข้อง ที่ต้องใช้ในการฝึกอบรม พร้อมทั้งสนับสนุนเอกสารและวัสดุที่ใช้ในการฝึกอบรมให้กับผู้เข้าฝึกอบรม พร้อมทั้งบริการกาแฟ และอาหารว่าง โดยต้องจัดเตรียมให้เพียงพอต่อผู้เข้าฝึกอบรม โดยไม่มีค่าใช้จ่ายใด ๆ ทั้งสิ้น

4. ลิขสิทธิ์ Software

ผู้ที่ได้รับการคัดเลือกที่ได้เป็นคู่สัญญากับธนาคาร จะต้องเป็นผู้รับผิดชอบให้ธนาคารมีสิทธิโดยถูกต้อง อันชอบธรรมในการใช้ Software ที่เสนอและ/หรือ Software ที่จำเป็นต้องใช้ในระบบที่ได้ส่งมอบ ให้แก่ธนาคาร รวมถึงสิทธิ์การใช้งานสำหรับ Tool และ/หรือ Application ที่ใช้ในการดำเนินการในโครงการนี้ทั้งหมด จะต้องมอบให้เป็นของธนาคารอย่างถูกต้องตามกฎหมายจากเจ้าของลิขสิทธิ์ ในกรณีที่ผู้ที่ได้รับการคัดเลือกทำการแก้ไขและพัฒนาเพิ่มเติม Tool และ/หรือ Application นั้น (Customize & Development) ผู้ที่ได้รับการคัดเลือกต้องมอบให้เป็นลิขสิทธิ์ของธนาคารด้วย ทั้งการเป็นเจ้าของลิขสิทธิ์และการใช้งาน ซึ่งธนาคารสามารถดำเนินการอย่างไรก็ได้กับการแก้ไข และการพัฒนาเพิ่มเติม Tool และ/หรือ Application นั้น โดยผู้ที่ได้รับการคัดเลือกไม่สามารถเรียกร้องลิขสิทธิ์หรือเรียกร้องค่าใช้จ่ายเพิ่มเติมได้อีกในการกระทำกับ Tool และ/หรือ Application นั้น ๆ ทั้งที่มีลิขสิทธิ์อยู่แล้ว หรืออาจมีลิขสิทธิ์เกิดขึ้นภายหลัง

ธนาคารอาคารสงเคราะห์ให้ความสำคัญกับการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ธนาคารจึงได้กำหนดนโยบายคุ้มครองข้อมูลส่วนบุคคล โดยสามารถศึกษารายละเอียดที่ QR Code นี้