แบบ บก.06

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย การจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ แผนงานโครงการจัดซื้อระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) พร้อมจ้างบริการบำรุงรักษา และจ้างเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP)
2. หน่วยงานเจ้าของโครงการ ศูนย์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ธนาคารอาคารสงเคราะห์ สำนักงานใหญ่
3. วงเงินงบประมาณที่ได้รับจัดสรร 44,000,000.- บาท (สี่สิบสี่ล้านบาทถ้วน)
4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ ...- 20 พ.ย. 2567 ..... เป็นเงิน 44,000,000.- บาท (สี่สิบสี่ล้านบาทถ้วน) (รวมภาษีมูลค่าเพิ่มแล้ว)
5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
   5.1 สืบจากท้องตลาด จำนวน 3 บริษัท ได้แก่
   - บริษัท เบย์ คอมพิวติ้ง จำกัด (มหาชน)
   - บริษัท ดาต้าโปร คอมพิวเตอร์ ซิสเต็มส์ จำกัด
   - บริษัท แอ็ดวานซ์อินฟอร์เมชั่นเทคโนโลยี จำกัด (มหาชน)
6. รายชื่อผู้รับผิดชอบในการกำหนดค่าใช้จ่าย/ดำเนินการ/ขอบเขตดำเนินการ (TOR) (ตามบันทึกข้อความที่ ศม.147/2567 ลว. 16 ก.ย. 2567)

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)
โครงการจัดซื้อระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP)
พร้อมจ้างบริการบำรุงรักษา และจ้างเฝ้าระวังภัยคุกคามทาง
Web Application and API Protection (WAAP)

102-230/67

1. ความเป็นมา/เหตุผลและความจำเป็น

ความเจริญก้าวหน้าด้านเทคโนโลยีสารสนเทศและการสื่อสารในรูปแบบและเทคนิคใหม่ๆ เข้ามามีบทบาทมากขึ้นในขณะเดียวกันพบว่าปัญหาความไม่ปลอดภัยด้านเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามด้านไซเบอร์ที่เพิ่มมากขึ้นเช่นกัน และมีแนวโน้มที่จะขยายตัวเพิ่มขึ้นในทุกภาคส่วน ซึ่งอาจสร้างความเสียหายให้กับธนาคารได้อย่างมาก ดังนั้นธนาคารจึงมีความจำเป็นต้องจัดซื้อระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) พร้อมจ้างบริการบำรุงรักษา และจ้างเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) (ทดแทนของเดิมที่จะหมดอายุการใช้งานและมีการใช้งานมาแล้ว 8 ปี) เพิ่มประสิทธิภาพการเฝ้าระวังการโจมตีทางไซเบอร์รูปแบบต่างๆ ที่มีผลกระทบกับการดำเนินงานของระบบสารสนเทศของธนาคาร

2. วัตถุประสงค์

2.1 เพื่อให้ธนาคารสามารถ ติดตาม เฝ้าระวัง และป้องกันภัยคุกคามทางไซเบอร์ต่างๆ ที่เกิดขึ้นกับ Web Application และ API ในระบบงานของธนาคาร

2.2 เพื่อให้ธนาคารสามารถนำข้อมูลการโจมตีทางไซเบอร์ต่างๆ และนำมาใช้ในการวิเคราะห์ และปรับปรุงระบบป้องกันของธนาคารได้

2.3 เพื่อให้ธนาคารสามารถบริหารจัดการภัยคุกคามทางไซเบอร์ต่างๆ ที่เกิดขึ้นกับ Web Application และ API ในระบบงานของธนาคารได้อย่างมีประสิทธิภาพ

3. คุณสมบัติของผู้เสนอราคา

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตาม

ระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้าง และการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพตามที่ประกวดราคาดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ธนาคาร ณ วันประกาศประกวดราคา หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e – GP) ของกรมบัญชีกลาง

3.11 ผู้ยื่นข้อเสนอต้องไม่เคยถูกยกเลิกสัญญาซื้อขาย หรือสัญญาจ้างบริการบำรุงรักษาฯ ก่อนหมดอายุสัญญา โดยไม่มีเหตุผลอันควรจากธนาคาร หรือหน่วยงานใดๆ

3.12 ผู้ยื่นข้อเสนอทุกรายจะต้องเก็บรักษาข้อมูลที่เกี่ยวข้องทั้งหมดของธนาคารไว้เป็นความลับ จะไปเผยแพร่ที่อื่นมิได้

3.13 ผู้ยื่นข้อเสนอต้องมีประสบการณ์ที่มีผลงานประเภทเดียวกันกับงานที่จะจัดซื้อจัดจ้างครั้งนี้ ให้กับองค์กรภาครัฐหรือเอกชนในประเทศไทย ที่มีมูลค่าโครงการไม่น้อยกว่า 14,000,000.- บาท (สิบสี่ล้านบาทถ้วน) ต้องเป็นผลงานในสัญญาเดียวและเป็นสัญญาที่ได้ทำงานแล้วเสร็จ ซึ่งได้มีการส่งมอบงานและตรวจรับเรียบร้อยแล้ว โดยผู้ยื่นข้อเสนอต้องแจ้งชื่อองค์กรหรือหน่วยงานดังกล่าว พร้อมสถานที่ติดตั้ง หมายเลขโทรศัพท์ผู้ติดต่อให้ธนาคารทราบ เพื่อให้สามารถติดต่อได้

3.14 ผู้ยื่นข้อเสนอต้องมีหนังสือรับรองมาแสดงต่อธนาคารเพื่อยืนยันว่าฮาร์ดแวร์และซอฟต์แวร์ ที่เสนอขายแก่ธนาคารต้องเป็นรุ่นที่ยังอยู่ในสายการผลิต สำหรับฮาร์ดแวร์ต้องเป็นเครื่องใหม่ที่เพิ่งผลิตจากโรงงานผู้ผลิตและยังไม่เคยติดตั้งใช้งานอื่นใดมาก่อน หากภายหลังเจ้าของผลิตภัณฑ์มีความจำเป็นต้องยุติการผลิต หรือเลิกการสนับสนุนฮาร์ดแวร์ที่เสนอ ผู้ยื่นข้อเสนอต้องมีหนังสือยืนยันสนับสนุนการบำรุงรักษา ฮาร์ดแวร์ ที่ธนาคารได้จัดหาและใช้งานอยู่ใน

ขณะนั้นให้แก่ธนาคารต่อไปอีกไม่น้อยกว่า 5 ปี นับแต่วันที่ธนาคาร (โดยคณะกรรมการตรวจรับ หรือ เจ้าหน้าที่ที่ได้รับแต่งตั้งมอบหมายให้ทำหน้าที่ตรวจรับได้) ตรวจรับมอบอุปกรณ์ที่ซื้อขายถูกต้องครบถ้วนเรียบร้อยแล้ว

3.15 ผู้ยื่นข้อเสนอต้องมีผู้เชี่ยวชาญในการเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) โดยมีใบรับรอง (Certified) CompTIA CASP+ หรือ CYSA+ หรือ CISSP (Certified Information System Security Professional) อย่างใดอย่างหนึ่งหรือมากกว่า โดยมีอายุของใบรับรองคงเหลือไม่น้อยกว่า 1 ปี นับถัดจากวันยื่นเอกสาร

3.16 ผู้ยื่นข้อเสนอต้องทำความเข้าใจในเอกสารทุกฉบับให้เป็นที่เข้าใจโดยชัดแจ้ง และไม่ว่ากรณีใดๆผู้ยื่นข้อเสนอจะยกขึ้นเป็นข้ออ้างโดยอาศัยเหตุจากการที่ละเลย ไม่ทำความเข้าใจในข้อความดังกล่าว หรือละเลยไม่ปฏิบัติตามข้อความนั้น หรือโดยอ้างความสำคัญผิดในความหมายของข้อความในใบเสนอราคาเพื่อปฏิเสธความรับผิดชอบมิได้

3.17 หากธนาคารพบหรือทราบเมื่อใดก็ตามว่า ผู้ยื่นข้อเสนอมีเจตนาที่จะปิดบัง บิดเบือน หรือพยายามให้ธนาคารเข้าใจผิดไปจากความเป็นจริง ธนาคารจะพิจารณาตัดสิทธิในการเสนอราคา หรือ ยกเลิกสัญญา ที่ได้ทำไว้กับผู้ยื่นข้อเสนอ และเรียกค่าเสียหายที่พึงเกิดขึ้นจากการกระทำดังกล่าว

3.18 ผู้ยื่นข้อเสนอต้องยืนยันว่าพร้อมที่จะลงนามในสัญญาตามแบบสัญญาของธนาคาร รวมทั้งเงื่อนไขต่างๆ ในการจัดซื้อระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) พร้อมจ้างบริการบำรุงรักษา และจ้างเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) ของธนาคาร ข้อเสนอของผู้ยื่นข้อเสนอรวมทั้งข้อเสนอเพิ่มเติมในการต่อรองให้ถือเป็นส่วนหนึ่งของสัญญาด้วย

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 ให้ยื่นสำเนาสัญญาของการเข้าร่วมค้า สำเนาบัตรประจำตัวประชาชนของผู้ร่วมค้า และในกรณีที่ผู้เข้าร่วมค้าฝ่ายใดเป็นบุคคลธรรมดาที่มิใช่สัญชาติไทย ก็ให้ยื่นสำเนาหนังสือเดินทาง หรือผู้ร่วมค้าฝ่ายใดเป็นนิติบุคคลให้ยื่นเอกสารตามที่ระบุไว้ใน (1)

(4) บัญชีเอกสารส่วนที่ 1 ทั้งหมดที่ได้ยื่นพร้อมกับซองใบเสนอราคา

4.2 ส่วนที่ 2 อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(1) แค็ตตาล็อกหรือแบบรูปรายละเอียดคุณลักษณะเฉพาะ

(2) ตารางเปรียบเทียบคุณลักษณะเฉพาะของระบบจัดเก็บบันทึกและวิเคราะห์เหตุการณ์ที่เสนอกับคุณลักษณะเฉพาะที่ธนาคารกำหนด

(3) หนังสือมอบอำนาจซึ่งปิดอากรแสตมป์ตามกฎหมายในกรณีที่ผู้ยื่นข้อเสนอราคามอบอำนาจ ให้บุคคลอื่นลงนามในใบเสนอราคาแทน

(4) บัญชีเอกสารส่วนที่ 2 ทั้งหมดที่ได้ยื่นพร้อมกับซองใบเสนอราคา

5. คุณลักษณะเฉพาะของพัสดุ

ผู้ยื่นข้อเสนอต้องนำเสนอระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) พร้อมจ้างบริการบำรุงรักษา และจ้างเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) เป็นระยะเวลา 5 ปี (รับประกัน 1 ปี, บำรุงรักษา 4 ปี และเฝ้าระวังภัยคุกคามฯ 5 ปี) โดยมีรายละเอียด และคุณลักษณะเฉพาะตามเอกสารแนบ

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 ธนาคารสงวนสิทธิ์ที่จะยกเลิกการจ้าง และพิจารณาแจ้งเป็นผู้ทิ้งงาน

8. รายละเอียดของงานที่จะจัดซื้อจัดจ้าง

ผู้ยื่นข้อเสนอต้องนำเสนอระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) พร้อมจ้างบริการบำรุงรักษา และจ้างเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) โดยมีรายละเอียดของงาน ตามเอกสารแนบ

9. ระยะเวลาดำเนินการ

9.1 <u>สัญญาซื้อขาย</u>

ระยะเวลาดำเนินการ/ส่งมอบระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) ภายใน 120 วัน นับถัดจากวัน ลงนามในสัญญาซื้อขาย เมื่อคณะกรรมการตรวจรับได้ตรวจรับมอบ แล้วเห็นว่าถูกต้อง ตรงตามเงื่อนไขของสัญญาซื้อขายเรียบร้อยแล้ว โดยมีเงื่อนไขการส่งมอบพัสดุ ตามเอกสารแนบ

9.2 <u>สัญญาจ้างบริการบำรุงรักษาฯ</u>

ระยะเวลาการว่าจ้างบริการบำรุงรักษาระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) เป็นเวลา 4 ปี หลังพ้นระยะเวลารับประกันของสัญญาซื้อขาย (ตามรายละเอียดระยะเวลาดำเนินการ ข้อ 9.1)

9.3 <u>สัญญาจ้างบริการเฝ้าระวังภัยคุกคามฯ</u>

ระยะเวลาการว่าจ้างบริการเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) เป็นเวลา 5 ปี (นับถัดจากวันที่ธนาคารได้ตรวจรับมอบ ระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) ตามสัญญาซื้อขาย ข้อ 9.1 เรียบร้อยแล้ว) โดยมีเงื่อนไขการดำเนินงาน ตามเอกสารแนบ

10. วงเงินที่จะจัดซื้อจัดจ้าง

วงเงินงบประมาณ 44,000,000.- บาท (สี่สิบสี่ล้านบาทถ้วน)

11. เงื่อนไขการชำระเงิน

ระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) พร้อมจ้างบริการบำรุงรักษา และจ้างบริการเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) หลังจากที่ได้ตรวจรับการส่งมอบงานถูกต้องครบถ้วนเรียบร้อยตามเงื่อนไขสัญญาที่ธนาคารกำหนด จะชำระเงินตามเงื่อนไข ดังนี้

11.1 สัญญาซื้อขาย

ธนาคารจะชำระเงินค่าจัดซื้อระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) ที่ส่งมอบเป็นรายงวด ชำระเงิน แบ่งเป็น 2 งวด ดังนี้

งวดที่ 1 **(ภายใน 90 วัน นับถัดจากวัน ลงนามในสัญญาซื้อขาย)**
จำนวน 40% ของมูลค่าตามสัญญา เมื่อผู้ได้รับการคัดเลือกดำเนินการจัดส่งอุปกรณ์/เครื่องแม่ข่าย ตามเอกสารแนบ เรียบร้อยแล้ว และคณะกรรมการตรวจรับได้ตรวจรับมอบแล้วเห็นว่าถูกต้อง ตรงตามเงื่อนไขของสัญญาซื้อขาย

งวดที่ 2 **(ภายใน 120 วัน นับถัดจากวัน ลงนามในสัญญาซื้อขาย)**
จำนวน 60% ของมูลค่าตามสัญญา เมื่อผู้ได้รับการคัดเลือกดำเนินการติดตั้งอุปกรณ์/เครื่องแม่ข่าย/ลิขสิทธิ์ซอฟต์แวร์ (License) และดำเนินการตั้งค่า เพื่อให้ระบบงานสามารถทำงานได้อย่างมีประสิทธิภาพตามเอกสารแนบ เรียบร้อยแล้ว และคณะกรรมการตรวจรับได้ตรวจรับมอบแล้วเห็นว่าถูกต้อง ตรงตามเงื่อนไขของสัญญาซื้อขาย

11.2 สัญญาจ้างบริการบำรุงรักษาฯ

ธนาคารจะชำระเงินค่าจ้างบริการบำรุงรักษาและซ่อมแซมแก้ไขระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) เป็นรายงวด (งวดละ 3 เดือน รวม 16 งวด) เมื่อคณะกรรมการตรวจรับของธนาคาร ได้ตรวจรับมอบในแต่ละงวดถูกต้องเรียบร้อยแล้ว

11.3 สัญญาจ้างบริการเฝ้าระวังภัยคุกคามฯ

ธนาคารจะชำระเงินค่าจ้างบริการเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) เป็นรายงวด (งวดละ 3 เดือน รวม 20 งวด) เมื่อคณะกรรมการตรวจรับของธนาคาร ได้ตรวจรับมอบในแต่ละงวดถูกต้องเรียบร้อยแล้ว

12. อัตราค่าปรับ

12.1 สัญญาซื้อขาย

กำหนดค่าปรับเป็นรายวันในอัตราร้อยละ 0.20 ของราคาพัสดุที่ยังไม่ได้รับมอบ

12.2 สัญญาจ้างบริการบำรุงรักษาฯ

กำหนดค่าปรับเป็นรายวันในอัตราร้อยละ 0.10 ของค่าจ้างบริการบำรุงรักษาฯ (รายงวด) ตามสัญญา

12.3 สัญญาจ้างบริการเฝ้าระวังภัยคุกคามฯ

กำหนดค่าปรับเป็นรายวันในอัตราร้อยละ 0.10 ของค่าจ้างบริการเฝ้าระวังภัยคุกคามฯ (รายงวด) ตามสัญญา

13. การรับประกันความชำรุดบกพร่อง

ผู้ได้รับการคัดเลือกต้องรับประกันให้ธนาคารสามารถใช้ปฏิบัติงานระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) ได้เป็นอย่างดีเป็นระยะเวลา 1 ปี นับถัดจากวันที่ธนาคารได้ตรวจรับมอบโดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น และในระหว่างระยะเวลาการรับประกันดังกล่าวให้นำเงื่อนไขการบำรุงรักษาระบบงานตามเอกสารแนบมาบังคับใช้โดยอนุโลม

14. ข้อสงวนสิทธิ์ในการยื่นข้อเสนอและอื่น ๆ (ถ้ามี)

14.1 เมื่อธนาคารได้คัดเลือกผู้ยื่นข้อเสนอรายใดให้เป็นผู้ขาย และได้ตกลงซื้อสิ่งของตามการดำเนินการจัดซื้อจัดจ้างแล้ว ถ้าผู้ขายจะต้องสั่งหรือนำสิ่งของดังกล่าวเข้ามาจากต่างประเทศและของนั้นต้องนำเข้ามาโดยทางเรือในเส้นทางที่มีเรือไทยเดินอยู่ และสามารถให้บริการรับขนได้ตามที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศกำหนด ผู้ยื่นข้อเสนอซึ่งเป็นผู้ขายจะต้องปฏิบัติตามกฎหมายว่าด้วยการส่งเสริมการพาณิชยนาวี ดังนี้

(1) แจ้งการสั่งหรือนำสิ่งของที่ซื้อขายดังกล่าวเข้ามาจากต่างประเทศต่อกรมเจ้าท่าภายใน 7 วัน นับตั้งแต่วันที่ผู้ขายสั่ง หรือซื้อของจากต่างประเทศ เว้นแต่เป็นของที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่นได้

(2) จัดการให้สิ่งของที่ซื้อขายดังกล่าวบรรทุกโดยเรือไทย หรือเรือที่มีสิทธิเช่นเดียวกับเรือไทย จากต่างประเทศมายังประเทศไทย เว้นแต่จะได้รับอนุญาตจากกรมเจ้าท่า ให้บรรทุกสิ่งของนั้นโดยเรืออื่นที่มิใช่เรือไทย ซึ่งจะต้องได้รับอนุญาตเช่นนั้นก่อนบรรทุก

ของลงเรืออื่น หรือเป็นของที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่น

(3) ในกรณีที่ไม่ปฏิบัติตาม (1) หรือ (2) ผู้ขายจะต้องรับผิดตามกฎหมายว่าด้วยการส่งเสริมการพาณิชยนาวี

14.2 ผู้ยื่นข้อเสนอซึ่งธนาคารได้คัดเลือกแล้ว ไม่ไปทำสัญญาหรือข้อตกลงซื้อเป็นหนังสือภายในเวลาที่กำหนด ดังระบุไว้ในข้อ 7 ธนาคารจะริบหลักประกันการยื่นข้อเสนอ หรือเรียกร้องจากผู้ออกหนังสือค้ำประกันการยื่นข้อเสนอทันที และอาจพิจารณาเรียกร้องให้ชดใช้ความเสียหายอื่น (ถ้ามี) รวมทั้งจะพิจารณาให้เป็นผู้ทิ้งงาน ตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ.2560

14.3 ธนาคารสงวนสิทธิ์ที่จะแก้ไขเพิ่มเติมเงื่อนไข หรือข้อกำหนดในแบบสัญญาหรือข้อตกลงซื้อเป็นหนังสือ ให้เป็นไปตามความเห็นของสำนักงานอัยการสูงสุด (ถ้ามี)

14.4 ในกรณีที่เอกสารแนบท้ายเอกสารประกวดราคาอิเล็กทรอนิกส์นี้ มีความขัดหรือแย้งกัน ผู้ยื่นข้อเสนอจะต้องปฏิบัติตามคำวินิจฉัยของธนาคาร คำวินิจฉัยดังกล่าวให้ถือเป็นที่สุด และผู้ยื่นข้อเสนอไม่มีสิทธิเรียกร้องค่าใช้จ่ายใดๆ เพิ่มเติม

14.5 ธนาคารอาจประกาศยกเลิกการจัดซื้อในกรณีต่อไปนี้ได้ โดยที่ผู้ยื่นข้อเสนอจะเรียกร้องค่าเสียหายใดๆ จากธนาคารไม่ได้

(1) ธนาคารไม่ได้รับการจัดสรรเงินที่จะใช้ในการจัดซื้อหรือที่ได้รับจัดสรรแต่ไม่เพียงพอที่จะทำการจัดซื้อครั้งนี้ต่อไป

(2) มีการกระทำที่เข้าลักษณะผู้ยื่นข้อเสนอที่ชนะการจัดซื้อหรือที่ได้รับการคัดเลือกมีผลประโยชน์ร่วมกัน หรือมีส่วนได้เสียกับผู้ยื่นข้อเสนอรายอื่น หรือขัดขวางการแข่งขันอย่างเป็นธรรม หรือสมยอมกันกับผู้ยื่นข้อเสนอรายอื่น หรือเจ้าหน้าที่ในการเสนอราคา หรือส่อว่ากระทำการทุจริตอื่นใดในการเสนอราคา

(3) การทำการจัดซื้อครั้งนี้ต่อไปอาจก่อให้เกิดความเสียหายแก่ธนาคาร หรือกระทบต่อประโยชน์สาธารณะ

(4) กรณีอื่นในทำนองเดียวกับ (1) (2) หรือ (3) ตามที่กำหนดในกฎกระทรวง ซึ่งออกตามความในกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ

15. การปฏิบัติตามกฎหมายและระเบียบ

ในระหว่างระยะเวลาการซื้อ/จ้าง ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้รับจ้างต้องปฏิบัติตามหลักเกณฑ์ที่กฎหมายและระเบียบได้กำหนดไว้โดยเคร่งครัด

16. หน่วยงานที่รับผิดชอบ

ศูนย์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โทร. 02-202-1735

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

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

ลงชื่อ.....กรรมการ
(นายฉนานนท์ ตันสกุล)
พนักงานคอมพิวเตอร์อาวุโส

ลงชื่อ.....กรรมการ
(นายเอกณัฏฐ์ อเนกเจริญวณิช)
พนักงานด้านความมั่นคงปลอดภัยเทคโนโลยี
สารสนเทศอาวุโส

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

ลงชื่อ.....กรรมการและเลขานุการ
(นายธีระชัย วิสุทธิพันธ์)
ผู้ช่วยหัวหน้าส่วน

เอกสารแนบ

รายละเอียดและคุณลักษณะเฉพาะของโครงการจัดซื้อ

ระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP)

พร้อมจ้างบริการบำรุงรักษา และจ้างเฝ้าระวังภัยคุกคามทาง

Web Application and API Protection (WAAP)

---

1. คุณลักษณะเฉพาะของระบบงาน

ระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) พร้อมจ้างบริการบำรุงรักษา และจ้างเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) ที่ธนาคารต้องการจัดหา ประกอบด้วย 5 ส่วนหลัก ดังนี้

1. จัดหาและติดตั้งระบบป้องกันการโจมตี Web Application สำหรับศูนย์คอมพิวเตอร์หลัก (DC) จำนวน 1 ระบบ (สัญญาซื้อขาย)
2. จัดหาระบบป้องกันการโจมตีสำหรับ Web Application และ API โดยใช้ Cloud จำนวน 1 ระบบ (สัญญาซื้อขาย)
3. จัดหาและติดตั้งระบบคัดกรองและสำเนาข้อมูลจากระบบเครือข่าย (Network Packet Broker) จำนวน 1 ระบบ (สัญญาซื้อขาย)
4. ดำเนินการ Migration จากระบบงานเดิม (WAF) ไปใช้งานระบบที่นำเสนอ (สัญญาซื้อขาย)
5. ดำเนินการเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (สัญญาจ้างบริการเฝ้าระวังภัยคุกคามฯ)

โดยต้องสามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ โดยมีคุณสมบัติไม่ต่ำกว่าข้อกำหนดดังต่อไปนี้

1. จัดหาและติดตั้งระบบป้องกันการโจมตี Web Application สำหรับศูนย์คอมพิวเตอร์หลัก (DC) จำนวน 1 ระบบ ซึ่งประกอบด้วย (สัญญาซื้อขาย)

1.1 อุปกรณ์ Web Application Firewall แบบ Hardware Appliance จำนวน 2 เครื่อง มีคุณสมบัติอย่างน้อยดังนี้

1.1.1 ผลิตภัณฑ์ที่นำเสนอจะต้องได้รับการจัดอันดับด้าน Web Application Firewall หรือ Web Application and API Protection จาก Gartner Magic Quadrant ในกลุ่ม Leader หรือ Challenges ในระหว่างปี 2020-2022 อย่างน้อยหนึ่งปี

1.1.2 อุปกรณ์ต้องมีค่าความสามารถประมวลผลข้อมูล (WAF Throughput) ตามเอกสารดาต้าชีทที่เปิดเผยแบบสาธารณะในเว็บไซต์ของเจ้าของผลิตภัณฑ์ เป็นค่าใช้งานจริง เมื่อเปิดใช้ WAF Policy แบบ out-of-the-box จะต้องมีค่า WAF Throughput อย่าง

น้อย 1 Gbps หรือ เป็นอุปกรณ์ประเภท Application Delivery Control หรือ Load Balancer จะต้องมีค่า Traffic Processing L7 Throughput อย่างน้อย 95 Gbps

1.1.3 อุปกรณ์จะต้องมีจุดเชื่อมต่อ network ชนิด 1G Copper หรือดีกว่า อย่างน้อย 8 พอร์ต

1.1.4 อุปกรณ์ต้องมี Hard Drive แบบ Dual hot-swap หรือเทียบเท่า ขนาด 4 TB เป็นอย่างน้อย

1.1.5 อุปกรณ์ต้องมี Power supply แบบ Dual hot-swap หรือเทียบเท่าเป็นอย่างน้อย

1.1.6 อุปกรณ์ต้องรองรับการการติดตั้งเพื่อทำงานในโหมดต่อไปนี้

1.1.6.1 โหมด In-Line (Bridge) Transparent โดยต้องสามารถทำ In-Line Bypass หรือ Failed-Open เมื่ออุปกรณ์มีปัญหาได้

1.1.6.2 โหมด Reverse Proxy

1.1.7 มีระบบ Dynamic Profiling หรือ Auto Policy Generation เพื่อเรียนรู้ Parameter, Method, Cookie และ URL ของ Website ได้อัตโนมัติ และสามารถทำเป็น Profile Policy เพื่อป้องกันการใช้งานนอกเหนือพฤติกรรมที่เรียนรู้ได้

1.1.8 มีความสามารถในการตรวจจับโดยใช้เทคนิค หรือวิธีการดังต่อไปนี้ เป็นอย่างน้อย

1.1.8.1 OWASP Top 10 (Web Application ปีล่าสุด)

1.1.8.2 SQL injection

1.1.8.3 Buffer Overflow

1.1.8.4 HTTP smuggling

1.1.8.5 Cross Site Scripting

1.1.8.6 Data Leakage

1.1.9 สามารถส่งข้อมูล Log แบบ Syslog ไปยังระบบ Centralized Log หรือ ระบบ SIEM ได้

1.1.10 สามารถป้องกันการโจมตีไปยัง API (Application Program Interface) ที่อยู่ในรูปแบบ JSON และ XML ได้เป็นอย่างน้อย

1.1.11 สามารถทำ Predefined Policy หรือ Signature สำหรับตรวจสอบและป้องกันภัยคุกคามและการโจมตีที่เป็นรู้จักกันอย่างดี (Well Known) หรือตามหมายเลข CVE ได้

1.1.12 มี Reputation Intelligence เพื่อใช้ตรวจสอบระดับความเสี่ยง, ประเภทการโจมตี และอุตสาหกรรมเป้าหมาย ที่เคยเกิดขึ้นจาก IP Address ที่ต้องการได้

1.1.13 ระบบที่นำเสนอจะต้องรองรับการใช้งานได้อย่างมีประสิทธิภาพตลอดระยะเวลาการใช้งานตามสัญญา 5 ปี หากพบปัญหาการใช้งานของระบบบมีความล้าช้าหรือผิดปกติ เช่น มีการใช้งาน CPU 100% หรืออื่น ๆ ที่เกี่ยวข้องกับอุปกรณ์ของระบบ ทางผู้ได้รับ

การคัดเลือกจะต้องวิเคราะห์และดำเนินการปรับปรุงแก้ไข หรือ เพิ่มเติมอุปกรณ์ เพื่อให้ระบบสามารถใช้งานได้อย่างมีประสิทธิภาพ

1.1.14 อุปกรณ์ฮาร์ดแวร์ที่เสนอต้องมีประสิทธิภาพ ตามที่เสนอในโครงการได้ โดยการทำ Load test หรือ Performance test ว่า CPU หรือ Memory อยู่ในระดับไม่เกิน 80% หากพบว่าผลการทดสอบไม่ตรงตามที่เสนอ ผู้เสนอราคาต้องทำการปรับปรุงแก้ไขให้อุปกรณ์ทำงานอยู่ในระดับปกติ

1.2 **<u>อุปกรณ์ Centralize Management สำหรับบริหารจัดการอุปกรณ์ความปลอดภัยสำหรับ Web Application Firewall จำนวน 1 เครื่อง มีคุณสมบัติอย่างน้อยดังนี้</u>**

1.2.1 อุปกรณ์ที่เสนอต้องเป็น Hardware Appliance หรือ เป็น Virtual Appliance/Software โดยหากเป็น Virtual Appliance/Software ผู้เสนอจะต้องจัดหาเครื่องแม่ข่ายพร้อมติดตั้ง Software ให้ทำงานได้ตามจุดประสงค์โดยไม่มีค่าใช้จ่ายเพิ่มเติม

1.2.2 อุปกรณ์ที่เสนอจะต้อง Network Interface แบบ Gigabits Copper จำนวน ไม่น้อยกว่า 2 พอร์ต

1.2.3 อุปกรณ์ต้องมีหน่วยความจำขนาด 128 GB และ Hard Drive แบบ Dual hot-swap ขนาด 4 TB เป็นอย่างน้อย

1.2.4 อุปกรณ์ต้องมี Power supply แบบ Dual hot-swap หรือเทียบเท่าเป็นอย่างน้อย

1.2.5 สามารถแสดง Security Event หรือ Attack Log ได้ผ่าน GUI

1.2.6 สามารถทำรายงานภัยคุกคามที่เกิดขึ้นได้

1.2.7 สามารถอัพเดทฐานข้อมูลช่องโหว่รูปแบบการโจมตี (Attack Signature) แบบ Schedule หรือ Automatic ได้

1.2.8 มี Dashboard หรือ บริการวิเคราะห์การโจมตีที่เกิดขึ้นโดยอัตโนมัติ (Analytics) ที่แสดงผลข้อมูลในเชิงวิเคราะห์ได้อย่างน้อยดังต่อไปนี้

1.2.8.1 จัดกลุ่มและบ่งบอกถึงประเภทการโจมตีที่เกิดขึ้น (Correlated incidents) พร้อมระบุระดับความรุนแรงของเหตุการณ์ (Severity)

1.2.8.2 ประเภทการโจมตี Web site (Violation types)

1.2.8.3 อัตราการป้องกันต่อการโจมตีที่เกิดขึ้น (Blocked rate)

1.2.8.4 แนวโน้มการโจมตีที่เกิดขึ้น (Event and Incident)

1.2.8.5 จัดอันดับ Website ที่ถูกโจมตีสูงสุด (Top attacked websites)

1.2.8.6 ข้อมูล CVE ที่เกี่ยวข้อง

1.2.8.7 สามารถเลือกดูข้อมูลในช่วงเวลาที่กำหนดโดยสามารถดูย้อนหลังได้ 90 วัน เป็นอย่างน้อย

2. จัดหาระบบป้องกันการโจมตีสำหรับ Web Application และ API โดยใช้ Cloud จำนวน 1 ระบบ ซึ่งมีคุณสมบัติทางเทคนิค ดังนี้ (สัญญาซื้อขาย)

2.1 <u>ระบบ Cloud Web Application และ Web DDoS มีคุณสมบัติอย่างน้อยดังนี้</u>

2.1.1 เป็นผลิตภัณฑ์ที่ถูกจัดให้อยู่ใน Leader Quadrant ของ Gartner Magic Quadrant Web Application and API Protection ปี 2022 หรือใหม่กว่า

2.1.2 มี Datacenter หรือ Scrubbing Center ทั่วโลกไม่น้อยกว่า 60 แห่งและอยู่ในประเทศไทยไม่น้อยกว่า 1 แห่ง

2.1.3 รองรับการใช้งาน Data transfer ไม่น้อยกว่า 150TB ต่อเดือน หรือ Clean-Bandwidth 150 Mbps แบบ 95 percentile ต่อเดือน

2.1.4 สามารถใช้งาน website ที่มี domain name ที่แตกต่างกันได้อย่างน้อย 90 Profile

2.1.5 สามารถป้องกันการโจมตีผ่านทาง website ตาม OWASP Top 10 (Web Application ปีล่าสุด) เช่น SQL injection, cross-site scripting, illegal resource access, และ remote file inclusion ได้

2.1.6 สามารถป้องกันการโจมตี DDoS attack Layer 3, Layer 4 และ Layer 7 ได้อัตโนมัติ

2.1.7 มีระบบ Bot Management โดยแยกกลุ่มของ Bots ที่เป็นกลุ่ม Good bots และกลุ่ม Bad bots ได้

2.1.8 สามารถทำ Client-Side Detection เพื่อ Monitor 3rd party malicious link หรือ script เพื่อเฝ้าระวังการโจรกรรมข้อมูลผู้ใช้งานผ่านหน้าเว็บไซต์

2.1.9 สามารถทำ Server Load Balancing และสามารถทำ Global Server Load Balancing เพื่อทำ Site Fail-over ได้

2.1.10 ระบบ Dashboard ต้องสามารถแสดงข้อมูล Traffic, Security และ Performance เช่น ประเทศต้นทางของผู้ใช้งาน และภัยคุกคามที่เกิดขึ้นกับเว็บไซต์ได้อย่างน้อย 90 วันย้อนหลัง

2.1.11 มีระบบหรือเสนอบริการฐานข้อมูล IP Reputation สำหรับค้นหา ประวัติ และความเสี่ยงของ IP ที่ต้องสงสัยได้ และสามารถป้องกัน Bad Reputation IP ตามระดับความเสี่ยง และประเภทของความเสี่ยงได้ เช่น TOR IP และ Anonymous Proxy IP

2.1.12 สามารถส่ง Log ผ่านทาง API หรือ SFTP Server หรือ AWS S3 เพื่อจัดเก็บ Log ร่วมกับระบบ SIEM ที่มีอยู่ได้

2.1.13 สามารถทำการ Modify Request Header (Header Rewrites) ได้

2.1.14 สามารถ Cache Content ที่เป็น Static Content ได้ และสามารถทำ Custom Cache Rule โดยระบุ URL ที่ต้องการได้

2.1.15 สามารถทำ Virtual Waiting Room จำนวนไม่น้อยกว่า 1 room เพื่อจัดทำระบบคิว เมื่อมีการใช้งานในปริมาณมาก

2.1.16 สามารถจัดเก็บ Audit Event หรือ Trail หรือ Admin Activity ได้ไม่น้อยกว่า 5 ปี

2.1.17 สามารถวิเคราะห์การโจมตีที่เกิดขึ้นโดยอัตโนมัติ (Analytics) ที่แสดงผลข้อมูลในเชิงวิเคราะห์ได้อย่างน้อย ดังต่อไปนี้

2.1.17.1 แสดงการจัดกลุ่มและบ่งบอกถึงประเภทการโจมตีที่เกิดขึ้น (Correlated incidents) พร้อมระบุระดับความรุนแรงของเหตุการณ์ (Severity)

2.1.17.2 แสดงรูปแบบการโจมตี และเครื่องมือที่ใช้โจมตี Web site (Violation and Attack tool types)

2.1.17.3 แสดงอัตราการป้องกันต่อการโจมตีที่เกิดขึ้น (Blocked rate)

2.1.17.4 แสดงแนวโน้มการโจมตีที่เกิดขึ้น (Event and Incident)

2.1.17.5 แสดงและจัดอันดับ Website ที่ถูกโจมตีสูงสุด (Top attacked websites)

2.1.17.6 สามารถวิเคราะห์การโจมตีร่วมกับอุปกรณ์ Web Application Firewall ที่นำเสนอได้

2.1.17.7 แสดงและเลือกดูข้อมูลในช่วงเวลาที่กำหนด โดยต้องสามารถดูย้อนหลังได้ไม่ต่ำกว่า 90 วัน

2.2 **<u>ระบบตรวจสอบ API Security และ Advance bot protection (HD-WAAP)</u>**

2.2.1 สามารถกำหนดและควบคุม API Schema บน HTTP Protocol ได้ เช่น New path, New Method และ New Parameter violation เป็นอย่างน้อย และสามารถใช้งานได้อย่างน้อย 600 ล้าน API request/ปี

2.2.2 สามารถ Discovery API โดยสามารถแสดงข้อมูล Host, API Endpoints, OWASP Top 10 (API ปีล่าสุด) และ API endpoints with sensitive data ได้

2.2.3 สามารถทำ Data Classification ได้ทั้งแบบ pre-defined และกำหนด Custom Value ของค่า Parameter name และ Data Value เพื่อระบุ Sensitive Data ที่ใช้งานผ่าน API ได้

2.2.4 เป็นระบบที่ให้บริการในรูปแบบคลาวด์หรือระบบโปรแกรมพร้อมอุปกรณ์ฮาร์ดแวร์

2.2.5 สามารถเก็บบันทึกกิจกรรมที่เกิดขึ้นกับ Web Application และ API ที่ใช้งานผ่านอุปกรณ์ WAF ตาม URL ที่สามารถกำหนดย้อนหลังได้อย่างน้อย 100 ล้านกิจกรรมต่อเดือน

2.2.6 สามารถตรวจสอบอุปกรณ์ต้นทางด้วย JavaScript เพื่อวิเคราะห์ fingerprint ของอุปกรณ์นั้น

2.2.7 สามารถเรียกดูข้อมูลได้แบบทันที ผ่านหน้าเว็บ GUI พร้อมมีระบบ Filtering การแสดงผลข้อมูล

2.2.8 สามารถแสดงผลในรูปแบบตาราง, กราฟแท่ง, กราฟรูปแบบอื่นๆ ได้

2.2.9 สามารถสร้าง Dashboard และ Widget เพื่อแสดงผลข้อมูลตามที่ต้องการได้

2.2.10 สามารถแสดงข้อมูล Timestamp ของกิจกรรมที่เกิดขึ้นในระดับวันที่ ชั่วโมง นาที วินาทีได้

2.2.11 สามารถแสดงข้อมูลเชิงปริมาณแยกตามแต่ละ Website domain ได้โดยกำหนดเป็น Top Destination URL, Top Client IP address, Top User Agent Name และมีข้อมูลดังต่อไปนี้แสดงเป็นรายละเอียดประกอบดังนี้

2.2.11.1 User Agent Name

2.2.11.2 User Agent Version

2.2.11.3 OS Name

2.2.11.4 OS Version

2.2.11.5 Client IP address

2.2.11.6 Organization Name

2.2.11.7 Custom Header Name

2.2.11.8 Requested Path

2.2.11.9 Header Referrer

2.2.11.10 HTTP Method

3. **จัดหาและติดตั้งระบบคัดกรองและสำเนาข้อมูลจากระบบเครือข่าย (Network Packet Broker) จำนวน 1 ระบบ ซึ่งประกอบด้วย (สัญญาซื้อขาย)**

3.1 **<u>อุปกรณ์ Network Packet Broker จำนวน 2 เครื่อง มีคุณสมบัติอย่างน้อยดังนี้</u>**

3.1.1 เป็นอุปกรณ์ที่ถูกออกแบบมาใช้สำหรับทำสำเนาคัดกรองข้อมูลจากเครือข่าย และ ทำการส่งข้อมูลไปยังอุปกรณ์วิเคราะห์ข้อมูล โดยเฉพาะ (Visibility Appliance หรือ Network Packet Brokers)

3.1.2 มี Interface ที่สามารถทำหน้าที่เป็น Network Port สำหรับ รับข้อมูลจากเครือข่าย (Inline Network) และ สำหรับส่งต่อข้อมูลไปยังอุปกรณ์วิเคราะห์ข้อมูล (Inline Tool)ได้

3.1.3 มี Interface แบบ SFP+ จำนวน 24 พอร์ตโดยสามารถรองรับ Module แบบ 1 Gb และ 10 Gb ได้ และมี Transceiver module แบบ 10G SFP+ Multimode มาอย่างน้อย จำนวน 24 โมดูล

3.1.4 มี Interface แบบ 10/100/1000 RJ-45 จำนวนไม่น้อยกว่า 16 พอร์ต

3.1.5 Inline Network Interface สามารถทำการบายพาสแบบกายภาพ (Physical Bypass) หรือแบบลอจิคัล (Logical Bypass) ได้

3.1.6 มี Interface สำหรับ Management Port แบบ 10/100/1000 RJ-45 จำนวนไม่น้อยกว่า 1 พอร์ต และมี Console Port จำนวนไม่น้อยกว่า 1 พอร์ต

3.1.7 มีประสิทธิภาพในการรองรับ Throughput ได้ไม่น้อยกว่า 600 Gbps

3.1.8 มีความสามารถในการทำ Network Flow Mapping สำหรับการส่งต่อข้อมูลให้กับอุปกรณ์วิเคราะห์ข้อมูลตามที่กำหนดได้

3.1.9 มีความสามารถในการทำ Packet Filtering โดยใช้เงื่อนไขได้อย่างน้อยดังนี้

3.1.9.1 IPv4/IPv6 Addresses

3.1.9.2 Application Port Number

3.1.9.3 VLAN IDs

3.1.10 มีความสามารถในการตรวจสอบสถานะของเครื่องมือวิเคราะห์ข้อมูล(Inline Tools) ด้วยการส่งสัญญาณฮาร์ตบีทแบบสองทิศทาง (Bidirectional heartbeat)

3.1.11 มีความสามารถในการส่งข้อมูลไปยังเครื่องมือวิเคราะห์ข้อมูล(Inline Tools) แบบ N+1 หรือ 1+1

3.1.12 มีความสามารถจัดการทราฟฟิคที่ส่งผ่านได้โดยการทำ การรวมทราฟฟิก (Aggregation Traffic) หรือ ทำสำเนาทราฟฟิก (Replication Traffic) ที่ได้รับ ไปยัง Tool port หรือ Monitor Port ได้

3.1.13 มีความสามารถในการถอดรหัส (Decryption) Traffic Encryption (SSL/TLS) แบบ Inline SSL Decrpytion โดยมีประสิทธิภาพในการรองรับ Throughput ได้สูงสุดที่ 2.8 Gbps และ ต้องรองรับ SSL/TLS versions ดังต่อนี้เป็นอย่างน้อย SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 และ TLS 1.3

3.1.14 สามารถทำ Role-based Access Control (RBAC) โดยใช้ฐานข้อมูล User Name/Password ที่เก็บอยู่บนตัวอุปกรณ์ หรือ ทำ User Authentication ร่วมกับ LDAP , Radius และ TACACS+ ได้

3.1.15 อุปกรณ์มีหน่วยจ่ายไฟสำรอง (Redundancy Power Supply) และสามารถถอดเปลี่ยนโดยไม่ปิดอุปกรณ์ได้ (Hot-swappable)

3.1.16 สามารถส่ง Log ไปยัง Central Log (Splunk) โดยใช้ Syslog ได้

3.1.17 สามารถติดตั้งเข้ากับ Rack ขนาด 19" ได้

3.1.18 เป็นอุปกรณ์ไฟฟ้าที่ได้รับการรับรองความปลอดภัยในการใช้งาน และการรับรองระดับสัญญาณรบกวนจาก UL, EN และ IEC

3.2 **<u>อุปกรณ์ Centralize Management สำหรับบริหารจัดการอุปกรณ์ Network Visibilty หรือ Network Packet Broker จำนวน 1 ระบบ</u>**

3.2.1 เป็น Centralized Management แบบ Hardware Appliance ที่สามารถบริหารและจัดการ Network Visibilty หรือ Network Packet Broker และเป็นผลิตภัณฑ์จากผู้ผลิตเดียวกับ Network Visibilty หรือ Network Packet Broker ที่นำเสนอ

3.2.2 สามารถจัดการ,ตรวจสอบ และการกำหนดค่าของนโยบายทราฟฟิกเพื่อที่ส่งต่อไปยังอุปกรณ์วิเคราะห์ข้อมูล (Monitoring Tools) ได้

3.2.3 มีหน้า Dashboard และสามารถปรับแต่ง (Custom) เพื่อดูสถานะการทำงานของอุปกรณ์ Network Visibilty หรือ Network Packet Broker ที่บริหารจัดการอยู่ได้ และสามารถ Export ออกมาเป็นรายงานในรูปแบบของ PDF หรือ HTML โดยสามารถกำหนดช่วงเวลาที่ต้องการให้สร้างและแสดงผลรายงานได้ (schedule report)

3.2.4 สามารถตั้งเวลาการ Backup Configuration ของอุปกรณ์ที่บริหารจัดการอยู่ได้

3.2.5 สามารถตั้งเวลาการ Upgrade firmware version ของอุปกรณ์ที่บริหารจัดการอยู่ได้

4. **ดำเนินการ Migration จากระบบงานเดิม (WAF) ไปใช้งานระบบที่นำเสนอ โดยมีลักษณะงานดังนี้ (สัญญาซื้อขาย)**

4.1 <u>รายละเอียดการดำเนินงาน ก่อนการ Migration</u>

4.1.1 ดำเนินการจัดทำเอกสาร Network Diagram ของระบบงานที่นำเสนอโดยละเอียด และมีรายละเอียดครบถ้วน และแสดงความสัมพันธ์กับระบบงานข้างเคียง ในลักษณะของ High Level และ Low Level Diagram เพื่อให้ธนาคารรับทราบ พิจารณา และเห็นชอบก่อนการติดตั้งระบบงาน (ตามคุณลักษณะเฉพาะของระบบงาน ข้อ 1 – 3)

4.1.2 ดำเนินการจัดทำเอกสาร รายงานผลการ Vulnerability Assessment เครื่องแม่ข่ายหรืออุปกรณ์ ที่นำมาติดตั้งในธนาคาร และดำเนินการแก้ไขประเด็นที่ตรวจพบ ให้ธนาคารรับทราบ และต้องได้รับการยินยอมจากทางธนาคารก่อนการติดตั้ง

4.1.3 ดำเนินการจัดทำเอกสาร รายงานผลการ Penetration Testing เครื่องแม่ข่ายหรืออุปกรณ์ ที่นำมาติดตั้งในธนาคาร และดำเนินการแก้ไขประเด็นที่ตรวจพบ ให้ธนาคารรับทราบ และต้องได้รับการยินยอมจากทางธนาคารก่อนการติดตั้ง

4.1.4 ดำเนินการจัดทำเอกสาร รายงานผลการทำ System Hardening (IT Security Baseline) เครื่องแม่ข่ายหรืออุปกรณ์ ที่นำมาติดตั้งในธนาคาร ให้ธนาคารรับทราบ ในกรณีที่เป็นอุปกรณ์ประเภท Hardware Appliance และไม่สามารถทำการ Hardening ได้ ต้องมีหนังสือยืนยันการตั้งค่าความปลอดภัยจากเจ้าของผลิตภัณฑ์มายืนยันให้กับธนาคาร และต้องได้รับการยินยอมจากทางธนาคารก่อนการติดตั้ง

4.1.5 ดำเนินการจัดทำเอกสาร Implementation Plan โดยต้องมีการแสดงรายละเอียดของวิธีการ ระยะเวลาในการดำเนินการ ผลกระทบที่อาจเกิด และแนวทางในการกู้คืนระบบ เพื่อให้ธนาคารพิจารณาและเห็นชอบก่อนดำเนินการ โดยมีรายละเอียดอย่างน้อย ดังนี้

4.1.5.1 วิธีการสำรองข้อมูล การตั้งค่า Configuration/Signature/Policies ระบบงานเดิม (WAF) ของธนาคาร

4.1.5.2 วิธีการในการ Migration การตั้งค่า Configuration/Signature/Policies จากระบบงานเดิม ไปยังระบบงานที่นำเสนอ

4.1.5.3 วิธีการในการตรวจสอบความถูกต้อง ครบถ้วนของระบบงานที่อยู่ภายใต้การป้องกันของระบบ WAF หลังการ Migration ไปยังระบบงานที่นำเสนอ

4.1.5.4 วิธีการในการตรวจสอบปัญหา และแนวทางในการกู้คืนระบบงาน หากทำการ Migration ไม่สำเร็จ

4.1.6 ดำเนินการจัดทำเอกสาร Checklist เพื่อใช้ตรวจสอบความพร้อม และความครบถ้วนก่อนการ Migration ให้กับทางธนาคารพิจารณา และนำไปใช้งานในขั้นตอนของการ Migration

4.1.7 ดำเนินการจัดทำเอกสาร แสดงขั้นตอนการทดสอบระบบงานสำคัญของธนาคารหลังจาก Migration จากระบบงานเดิม (WAF) ขึ้นระบบงานที่นำเสนอ โดยแผนที่นำเสนอต้องครอบคลุม Feature และ Function ที่สำคัญ โดยมีระบบงานที่กำหนด ดังนี้

4.1.7.1 ระบบงาน GHB ALL GEN

4.1.7.2 ระบบงาน GHB Line Buddy

4.1.7.3 ระบบงาน Exchange Mail

4.1.7.4 ระบบงาน Open Source Mail

4.1.7.5 ระบบงาน ghbhomecenter

4.1.7.6 ระบบงาน ghbank

4.1.8 ดำเนินการจัดทำเอกสาร แสดงรายละเอียดการทดสอบ Fail Over ในเหตุการณ์ที่อุปกรณ์ WAF Gateway สำหรับศูนย์คอมพิวเตอร์หลัก (DC) หยุดการทำงาน 1 ตัว โดยระบบที่นำเสนอ ต้องสามารถสลับการใช้งานไปยังอุปกรณ์ WAF Gateway อีกตัวได้อย่างอัตโนมัติและทำงานได้ต่อเนื่อง โดยไม่ทำให้ระบบที่อยู่ภายใต้การป้องกันหยุดการทำงาน

4.1.9 ดำเนินการจัดทำเอกสาร แสดงรายละเอียดการทดสอบเปลี่ยนการไหลของข้อมูล โดยการตั้งค่าผ่าน ระบบป้องกันการโจมตีสำหรับ Web Application และ API โดยใช้ Cloud ได้

4.2 **<u>รายละเอียดการดำเนินงานระหว่างการ Migration</u>**

4.2.1 ดำเนินการตั้งค่าระบบงานที่นำเสนอให้สามารถทำงานร่วมกับเว็บไซต์หรือ Application ที่อยู่ภายใต้การป้องกันของระบบที่นำเสนอหลังการ Migration ได้เป็นอย่างดี

4.2.2 ระบบงานที่นำเสนอต้องสามารถทำงานตามค่า Configuration/Signature/Policies ของระบบงานเดิมได้เป็นอย่างดี หากมีความจำเป็นต้องปรับเปลี่ยนค่าเพิ่มเติมเพื่อให้ระบบสามารถทำงานได้ ต้องแจ้งให้ธนาคารรับทราบก่อนการดำเนินการ

4.2.3 ดำเนินการทดสอบ Fail Over ในเหตุการณ์ที่อุปกรณ์ WAF Gateway สำหรับศูนย์คอมพิวเตอร์หลัก (DC) หยุดการทำงาน 1 ตัว โดยระบบที่นำเสนอ ต้องสามารถสลับการใช้งานไปยังอุปกรณ์ WAF Gateway อีกตัวได้อย่างอัตโนมัติและทำงานได้ต่อเนื่องโดยไม่ทำให้ระบบที่อยู่ภายใต้การป้องกันหยุดการทำงาน และสรุปรายงานผลการทดสอบในธนาคารรับทราบเป็นเอกสาร

4.2.4 ดำเนินการทดสอบเปลี่ยนการไหลของข้อมูล โดยการตั้งค่าผ่าน ระบบป้องกันการโจมตีสำหรับ Web Application และ API โดยใช้ Cloud ได้ และสรุปรายงานผลการทดสอบในธนาคารรับทราบเป็นเอกสาร

4.2.5 ในกรณีที่ระบบที่นำเสนอไม่สามารถทำงานร่วมกับของ Network Device เดิมของธนาคารได้ตามปกติ ทางบริษัทจะต้องจัดหาอุปกรณ์ มาใช้เพื่อให้ระบบที่นำเสนอสามารถทำงานร่วมกับ Network Device เดิมของธนาคารได้ โดยไม่มีค่าใช้จ่ายเพิ่มเติม

4.2.6 ดำเนินการตั้งค่าให้ระบบงานที่นำเสนอ ส่งข้อมูลจราจรทางคอมพิวเตอร์ (Log) ในรูปแบบ CEF Format หรือตามรูปแบบอื่นที่สามารถทำงานร่วมกับ Central Log (Splunk) ของธนาคารได้

4.2.7 ในกรณีที่ทางธนาคารต้องทำเรื่องเพื่อ แจ้งธนาคารแห่งประเทศไทย เพื่อปิดระบบในการ Migration ทางบริษัทต้องให้การสนับสนุนในการเตรียมเอกสารประกอบที่เกี่ยวข้องเพื่อใช้ในการขออนุมัติ

4.3 <u>รายละเอียดการดำเนินงานหลังการ Migration</u>

4.3.1 ดำเนินการจัดทำเอกสาร สรุปผลการนำระบบงานของธนาคาร ตามคุณลักษณะเฉพาะของระบบงานที่นำเสนอ

4.3.2 ดำเนินการจัดทำเอกสาร แสดงข้อมูลการตั้งค่าปัจจุบัน ของระบบงานที่นำเสนอ โดยต้องครอบคลุมในทุก Module ที่นำเสนอในโครงการ

4.3.3 ดำเนินการจัดทำเอกสาร User Matrix ของบัญชีผู้ใช้งานทั้งหมด ในระบบงานที่นำเสนอ ทั้งบัญชีผู้ใช้งาน OS, Application หรือส่วนอื่นๆ ที่เกี่ยวข้อง

4.3.4 ดำเนินการจัดทำ Dashboard ในระบบงาน Central Log (Splunk) ของธนาคาร โดยใช้ข้อมูล จากระบบที่นำเสนอ (Log ที่ธนาคารกำหนด) เพื่อใช้ตรวจสอบข้อมูล ดังนี้

4.3.4.1 Top 10 User Agent

4.3.4.2 Top 10 Attack Source

4.3.4.3 Top 10 Destination Website and Request Path per Hour

4.3.4.4 Summary Request Method per Hour

4.3.4.5 API Request

- Top API Request Path
- Top API Request Method
- Top API Request from IP Address
- Top API Request by User Agent

5. **ดำเนินการเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (สัญญาจ้างบริการเฝ้าระวังภัยคุกคามฯ)**

5.1 การเฝ้าระวังภัยคุกคามทาง Web Application and API Protection

5.1.1 ดำเนินการเฝ้าระวัง และแจ้งเตือนภัยคุกคาม ที่เกิดกับ ระบบงานของธนาคาร ที่อยู่ในระบบ Web Application Firewall and API Protection (WAAP) ตลอด 24 ชั่วโมง

5.1.2 ดำเนินการแจ้งเตือนเจ้าหน้าที่ของธนาคาร เมื่อพบเหตุการณ์ที่คาดการณ์ว่าจะเป็นลักษณะการโจมตีแบบ Targeted Attack หรือเป็นการโจมตีแบบมุ่งเป้ามาที่ธนาคาร จากข้อมูลของระบบที่นำเสนอ

5.1.3 กรณีที่เกิดการโจมตีที่เข้าข่ายรุนแรงระดับสูง หรือธนาคารต้องการข้อมูลเกี่ยวกับภัยคุกคามที่เกิดขึ้นในปัจจุบัน หรือตรวจพบกับระบบงานของธนาคารแบบละเอียด ธนาคารสามารถแจ้งให้จัดทำรายงานเชิงลึก เพิ่มเติมได้

5.1.4 จัดทำรายสรุปเหตุการณ์ภัยคุกคามประจำวัน (Daily Report) และส่งให้กับธนาคารผ่านทางอีเมล์ทุกวัน โดยมีรายละเอียดของรายงาน อย่างน้อยดังนี้

5.1.4.1 จำนวน Threat Event , Block Event และ High Severity Event ที่ตรวจพบในวัน

5.1.4.2 กราฟแสดงข้อมูล Threat Activities ในแต่ละช่วงเวลาของวัน เพื่อแสดงปริมาณการโจมตีในแต่ละช่วงเวลา

5.1.4.3 รายงานสรุปข้อมูล Top 10 Signature ของการโจมตีที่เกิดขึ้นกับระบบงานของธนาคารในแต่ละวัน

5.1.4.4 รายงานสรุปข้อมูล Top 10 Attacker ที่โจมตีระบบงานของธนาคารในแต่ละวัน

5.1.4.5 รายงานสรุปข้อมูล Top 10 Target (ระบบงานธนาคาร) ที่โดนโจมตีในแต่ละวัน

5.1.5 จัดทำรายงานและนำเสนอข้อมูลการเฝ้าระวังภัยคุกคาม แบบรายเดือน (Monthly Report) พร้อมประชุมนำเสนอกับเจ้าหน้าที่ของธนาคาร โดยมีหัวข้อ ดังนี้

5.1.5.1 จำนวน Threat Event , Block Event และ High Severity Event ที่ตรวจพบ

5.1.5.2 กราฟแสดงข้อมูล ภาพรวมการโจมตี ในแต่ละเดือนย้อนหลัง 6 เดือนล่าสุด

5.1.5.3 รายงานสรุปข้อมูล Top 10 Signature ของการโจมตีที่เกิดขึ้นกับระบบงานของธนาคาร ที่ตรวจพบในเดือนนั้น

5.1.5.4 รายงานสรุปข้อมูล Top 10 การโจมตี ของระบบงานที่ธนาคารสนใจ พร้อมทั้งแสดงข้อมูลรายละเอียดต่างๆ ของการโจมตี

5.1.5.5 รายงานสรุปข้อมูล Top 10 Attacker ที่โจมตีระบบงานของธนาคาร และถูกบล็อคในเดือน

5.1.5.6 รายงานสรุปข่าว Cyber Security News และแนวโน้มภัยคุกคามทาง Cyber Security ที่สำคัญประจำเดือน

5.2 การปรับปรุงการเฝ้าระวังภัยคุกคามทาง Web Application and API Protection

5.2.1 ดำเนินการสร้าง หรือ สนับสนุนการสร้าง Signature/Policies สำหรับตอบสนองต่อภัยคุกคามประเภท 0-day attack ที่เกิดบน Web Application and API Protection

5.2.2 ดำเนินการปรับแต่ง Signature/Policies เพื่อลด False Positive ให้เหมาะสมกับระบบงานของธนาคาร ผ่านทางช่องทางที่ธนาคารจัดหาให้ (Secure Channel) หลังจากได้รับแจ้ง หรือยืนยันผ่านทางอีเมล์, โทรศัพท์ หรือเป็นลายลักษณ์อักษรจากธนาคาร ภายในระยะเวลา 24 ชั่วโมง

5.2.3 กรณีเกิดเหตุการณ์ที่เข้าข่ายต้องสงสัย หรือเป็นพฤติกรรมที่อยู่ในความสนใจของธนาคาร ธนาคารสามารถแจ้งให้ ดำเนินการสร้าง หรือปรับแต่ง Signature/Policies ภายในอุปกรณ์ เพิ่มเติม เพื่อเก็บข้อมูลในเหตุการณ์ต่างๆ ที่รองรับได้ ภายในระยะเวลา 48 ชั่วโมง

2. เงื่อนไขการติดตั้งและส่งมอบ (สัญญาซื้อขาย)

2.1 ผู้ที่ได้รับการคัดเลือกต้องทำการสำรวจสถานที่ติดตั้งระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) ก่อนการดำเนินการติดตั้ง

2.2 ผู้ที่ได้รับการคัดเลือกต้องจัดส่ง เครื่องแม่ข่าย, อุปกรณ์, ซอฟต์แวร์ ระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) ที่ซื้อขาย ณ ธนาคารอาคารสงเคราะห์ สำนักงานใหญ่ (ตามคุณลักษณะเฉพาะของระบบงาน ข้อ 1-3) ให้ครบถ้วน ภายใน 90 วัน นับถัดจากวันที่ลงนามในสัญญาซื้อขาย

2.3 ผู้ที่ได้รับการคัดเลือกจะต้องดำเนินการติดตั้งระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) ที่ซื้อขายให้สามารถใช้งานได้ (ตามคุณลักษณะเฉพาะของระบบงาน ข้อ 1-4) ตามแผนการติดตั้งที่กำหนด และสามารถทำงานได้อย่างสมบูรณ์ให้ครบถ้วน ภายใน 120 วัน นับถัดจากวันที่ลงนามในสัญญาซื้อขาย

2.4 ในกรณีจำเป็นต้องดำเนินการเพื่อให้ระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) ที่ผู้ที่ได้รับการคัดเลือกเสนอสามารถต่อร่วมและใช้งานร่วมกับอุปกรณ์เดิมที่ธนาคารมีอยู่ได้อย่างสมบูรณ์ มีประสิทธิภาพสูงสุด ผู้ได้รับการคัดเลือกจะต้องเป็นผู้ดำเนินการด้วยค่าใช้จ่ายของผู้ได้รับการคัดเลือก ทั้งนี้ให้รวมถึงในกรณีที่ระบบที่เสนอต้องใช้เครื่องแม่ข่าย, อุปกรณ์, ซอฟต์แวร์ หรือสิทธิ์การใช้งาน (License) เพิ่มขึ้นจากที่ผู้ที่ได้รับการคัดเลือกเสนอ

2.5 ในระหว่างการดำเนินการ ไม่ว่าจะเป็นขั้นตอนของการสั่งซื้อ การทำสัญญา หรือการส่งของ ผู้ที่ได้รับการคัดเลือกมีเครื่องรุ่นใหม่ที่มีประสิทธิภาพดีกว่ารุ่นที่เสนอขายให้ธนาคาร และราคาขายต่อหน่วยเท่ากับหรือต่ำกว่า ผู้ที่ได้รับการคัดเลือกต้องแจ้งให้ธนาคารทราบเป็นลายลักษณ์อักษรและมีเครื่องพร้อมที่จะส่งมอบให้ธนาคาร ทั้งนี้ธนาคารสงวนสิทธิ์ที่จะพิจารณาเปลี่ยนแปลงหรือไม่เปลี่ยนแปลงก็ได้ และหากราคาขายต่ำกว่าเดิม ให้ใช้ราคาขายที่ต่ำกว่านั้นเป็นราคาที่ขายให้ธนาคาร

2.6 ผู้ที่ได้รับการคัดเลือกจะต้องจัดส่งเอกสาร (ตามที่กำหนดในคุณลักษณะเฉพาะของระบบงาน ข้อ 4) รวมถึงเอกสารอื่นๆ ที่เกี่ยวข้อง ของระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) ต้องถูกรวบรวมและส่งมอบ ในลักษณะของแฟ้มงาน จำนวน 1 แฟ้ม และจัดทำ Index ของเอกสาร แบ่งแยกเอกสารแต่ละชุดอย่างชัดเจนให้แก่ธนาคาร และส่งมอบไฟล์ (Soft File) ทั้งหมดใน USB

2.7 ผู้ที่ได้รับการคัดเลือกจะต้องส่งเจ้าหน้าที่ผู้เชี่ยวชาญเข้ามาศึกษาระบบภายในธนาคารที่เปิดให้บริการ พร้อมทั้งจัดทำรายงานนำเสนอให้เจ้าหน้าที่ที่ดูแลระบบรับทราบและยืนยันข้อมูล

2.8 ผู้ที่ได้รับการคัดเลือกจะต้องติดตั้ง พร้อมทั้งปรับแต่งระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เพื่อให้ทำงานร่วมกันได้เป็นอย่างดีกับระบบงานเดิมของธนาคารที่เปิดให้บริการ

2.9 ผู้ที่ได้รับการคัดเลือกจะต้องจัดให้มีเจ้าหน้าที่ ที่มีความเชี่ยวชาญด้านการบริหารจัดการระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) อย่างน้อย 1 ท่าน เพื่อสนับสนุน ให้คำแนะนำ ในลักษณะ On The Job Training เกี่ยวกับ ระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) ที่นำเสนอ โดยต้องเข้าปฏิบัติงานตั้งแต่ เวลา 08.30 – 16.30 น. (วันทำการ) เป็นเวลา 30 วัน ภายในระยะเวลา 1 ปี โดยธนาคารจะเป็นผู้กำหนดวันเข้ามาปฏิบัติงานที่ธนาคาร และแจ้งล่วงหน้าก่อนวันเข้าปฏิบัติงานจริง 3 วันทำการ เพื่อให้คำปรึกษาและดำเนินการปรับแต่ง แก้ไขค่า Configuration ของอุปกรณ์ที่เกี่ยวข้องเพื่อให้สามารถทำงานได้อย่างมีประสิทธิภาพ

2.10 ผู้ที่ได้รับการคัดเลือกจะต้องจัดหลักสูตรการฝึกอบรมให้แก่ผู้ดูแลระบบ ในการดูแลติดตั้งและงานใช้งานระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) ให้กับธนาคาร

3. **การบำรุงรักษา** Preventive Maintenance **(สัญญาจ้างบริการบำรุงรักษาฯ)**

3.1 ผู้ที่ได้รับการคัดเลือกจะต้องให้บริการซ่อมแซมแก้ไขระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) เมื่อผู้ขายได้รับแจ้งจากผู้ซื้อในวันจันทร์-วันศุกร์ เวลา 8.00 น. – 20.00 น. ทั้งนี้ผู้ที่ได้รับการคัดเลือกจะต้องเข้ามาดำเนินการซ่อมแซมแก้ไขให้กับธนาคารตามเงื่อนไขการให้บริการของสัญญา

3.2 ในการปฏิบัติการให้บริการตรวจดูแลบำรุงรักษา (Preventive Maintenance) ระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) แก่ธนาคารตามปกติแต่ละครั้ง ผู้ที่ได้รับการคัดเลือกต้องแจ้งกำหนดวันเวลาการมาให้บริการให้แก่ธนาคารได้ทราบเป็นลายลักษณ์อักษร/ทางจดหมายอิเล็กทรอนิกส์ (E-Mail) ล่วงหน้าไม่น้อยกว่า 3 วัน ทำการ ก่อนวันให้บริการ เพื่อธนาคารจะได้พิจารณาให้ความสะดวกในการให้บริการดังกล่าว และเพื่อมิให้เกิดปัญหาแก่การปฏิบัติงานของธนาคาร และจะต้องดำเนินการให้บริการตรวจดูแลบำรุงรักษาและซ่อมแซมแก้ไข ตามเงื่อนไขการให้บริการของสัญญา

3.3 ผู้ที่ได้รับการคัดเลือกจะต้องจัดให้ช่างผู้มีความรู้ความชำนาญและฝีมือดีมาตรวจสอบบำรุงรักษา อย่างน้อยเดือนละ 1 ครั้ง มิฉะนั้นผู้ที่ได้รับการคัดเลือกต้องยินยอมให้ธนาคาร คิดค่าปรับเป็นจำนวนเงินในอัตราร้อยละ 0.50 ของค่าจ้างบำรุงรักษา (รายงวด) ต่อการผิดเงื่อนไข

การให้บริการหนึ่งครั้ง แต่มูลค่ารวมของการปรับแต่ละครั้งต่ำสุด 500 บาท โดยมีเงื่อนไขการให้บริการดูแลรักษา ดังนี้

3.3.1 ตรวจสอบอุปกรณ์ที่ติดตั้งในโครงการนี้ทั้งหมดและอุปกรณ์ที่เกี่ยวข้องตามมาตรฐานของผู้ผลิต

3.3.2 ตรวจสอบ System เพื่อตรวจหาปัญหาต่างๆที่อาจพบได้และแก้ไขปัญหาให้เรียบร้อย

3.3.3 ตรวจสอบ Security Log

3.3.4 ตรวจสอบการทำงานและแก้ไขปัญหาให้เรียบร้อย

3.3.5 ตรวจสอบความเรียบร้อยของอุปกรณ์

3.3.6 ทำความสะอาดอุปกรณ์

3.3.7 ดูแลตรวจเช็คสภาพภายนอก

3.3.8 วิเคราะห์ Performance

3.3.9 สำรองข้อมูลค่า Configuration ของระบบ

3.3.10 ดำเนินการอื่นๆเพื่อให้อยู่ในสภาพพร้อมใช้งาน

3.3.11 ทำรายงานสรุปผลให้ทราบเป็นลายลักษณ์อักษรให้แก่หน่วยงานที่ดูแลเก็บไว้เป็นหลักฐาน

4. **การซ่อมแซมแก้ไข** Corrective Maintenance (**สัญญาจ้างบริการบำรุงรักษาฯ**)

ผู้ที่ได้รับการคัดเลือกต้องให้บริการซ่อมแซมแก้ไขในวันจันทร์-วันอาทิตย์ ตลอดเวลา 24 ชม. (7 x 24) กรณีเกิดความเสียหายชำรุดบกพร่องหรือเกิดเหตุขัดข้องอันเนื่องมาจากการใช้งานปกติ ผู้ที่ได้รับการคัดเลือกต้องดำเนินการการซ่อมแซมแก้ไข โดยมีเงื่อนไข ดังนี้

4.1 ผู้ที่ได้รับการคัดเลือกต้องเริ่มจัดการซ่อมแซมแก้ไขภายใน 2 ชั่วโมง นับตั้งแต่เวลาที่ได้รับแจ้งจากธนาคารหรือผู้ที่ได้รับมอบหมายจากธนาคาร โดยจะแจ้งให้ผู้ที่ได้รับการคัดเลือกหรือผู้ที่ได้รับมอบหมายจากผู้ที่ได้รับการคัดเลือกทราบทางวาจา ทางโทรสาร หรือทางจดหมายอิเล็กทรอนิกส์ (E-Mail) หรือทางโทรศัพท์ ไม่ว่าวิธีใดวิธีหนึ่งให้ถือเป็นการแจ้งโดยชอบตามสัญญานี้แล้ว และผู้ที่ได้รับการคัดเลือกจะต้องซ่อมแซมแก้ไข หรือเปลี่ยนสิ่งที่จำเป็นให้เสร็จเรียบร้อยภายใน 6 ชั่วโมง นับแต่เวลาที่ได้รับแจ้งจากธนาคารดังกล่าว

ในกรณีที่ผู้ที่ได้รับการคัดเลือกไม่เข้ามาซ่อมแซมแก้ไขภายในเวลาที่กำหนด หรือไม่สามารถดำเนินการซ่อมแซมแก้ไขหรือไม่สามารถจัดหาอุปกรณ์ใหม่ที่มีคุณสมบัติทัดเทียมกันหรือดีกว่ามาเปลี่ยนให้ใช้งานได้ ภายในเวลาที่กำหนดไว้ ผู้ที่ได้รับการคัดเลือกยินยอมให้คิดค่าปรับเป็น

รายชั่วโมง (เศษของชั่วโมงให้นับเป็น 1 (หนึ่ง) ชั่วโมง) ในอัตราร้อยละ 0.035 ของค่าจ้างบำรุงรักษา (รายงวด) ตามสัญญา นับจากเวลาที่ครบกำหนดจนถึงเวลาที่ผู้ที่ได้รับการคัดเลือกได้เริ่มการซ่อมแซมแก้ไข หรือจนถึงเวลาที่ผู้รับจ้างดำเนินการซ่อมแซมแก้ไขแล้วเสร็จแล้วแต่กรณี ทั้งนี้ หากผู้ที่ได้รับการคัดเลือกไม่ดำเนินการดังกล่าว ธนาคารมีสิทธิจ้างบุคคลภายนอกทำการซ่อมแซมแก้ไข โดยผู้ที่ได้รับการคัดเลือกจะต้องออกค่าใช้จ่ายในการจ้างบุคคลภายนอกซ่อมแซมแก้ไขแทนธนาคารทั้งสิ้น

4.2 หากผู้ที่ได้รับการคัดเลือกไม่อาจแก้ไขได้ ผู้ที่ได้รับการคัดเลือกจะต้องจัดหาอุปกรณ์ที่มีคุณภาพ ประสิทธิภาพและความสามารถในการใช้งานไม่ต่ำกว่าของเดิม ชดใช้แทนหรือชดใช้ราคาของ อุปกรณ์ในขณะที่เกิดความเสียหาย ในกรณีที่ไม่อาจจัดหาอุปกรณ์ดังกล่าวชดใช้แทนได้ให้แก่ธนาคารภายในเวลาที่ธนาคารกำหนด ผู้ที่ได้รับการคัดเลือกต้องยินยอมให้ธนาคารปรับเป็นรายวันในอัตราร้อยละ 0.01 ของค่าจ้างตามสัญญานี้

4.3 การใช้งานระบบเฝ้าระวังภัยคุกคามทาง Web Application and API Protection (WAAP) ตามสัญญานี้ให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอ โดยให้มีเวลาขัดข้องรวมตามเกณฑ์การคำนวณเวลาขัดข้อง ไม่เกินเดือนละ 72 ชั่วโมง หรือร้อยละ 10 ของเวลาใช้งานทั้งหมดของเดือนนั้น แล้วแต่ตัวเลขใดจะมากกว่ากัน มิฉะนั้นผู้ที่ได้รับการคัดเลือกต้องยินยอมให้ธนาคารคิดค่าปรับเป็นรายชั่วโมง ในอัตราร้อยละ 0.035 ของค่าจ้างบำรุงรักษา (รายงวด) ตามสัญญา ในช่วงเวลาที่ไม่สามารถใช้คอมพิวเตอร์ได้ในส่วนที่เกินกว่ากำหนดเวลาขัดข้องข้างต้น

5. การฝึกอบรม (สำหรับสัญญาซื้อขาย)

ผู้ที่ได้รับการคัดเลือกต้องจัดการฝึกอบรมให้แก่ผู้เข้าฝึกอบรมของธนาคารภายในเวลา 120 วัน นับถัดจากวันลงนามในสัญญาซึ่งมีหัวข้อของหลักสูตรที่ครอบคลุมทั้งภาคทฤษฎีและภาคปฏิบัติอย่างน้อย ดังนี้

ที่	ชื่อหลักสูตร	จำนวนวัน	สถานที่อบรม	จำนวนครั้ง	จำนวนคนต่อครั้ง
1	Hardware Solution	1	ธนาคารอาคาร	1	7
2	System & Configuration	1	สงเคราะห์	1	7
3	Administration การใช้งานและการดูแลระบบ	2	(สำนักงานใหญ่) หรือตามที่ธนาคารกำหนด	1	7

ทั้งนี้ การฝึกอบรมทุกครั้ง ผู้ที่ได้รับการคัดเลือกจะต้องเป็นผู้ดำเนินการจัดหาติดตั้งอุปกรณ์ที่เกี่ยวข้องที่ต้องใช้ในการฝึกอบรม พร้อมทั้งสนับสนุนเอกสารและวัสดุที่ใช้ในการฝึกอบรมให้กับผู้เข้าฝึกอบรม พร้อมทั้งบริการกาแฟ และอาหารว่าง โดยต้องจัดเตรียมให้เพียงพอต่อผู้เข้าฝึกอบรม โดยไม่มีค่าใช้จ่ายใด ๆ ทั้งสิ้น

6. คู่มือ (สัญญาซื้อขาย)

ผู้ที่ได้รับการคัดเลือกต้องจัดส่งเอกสาร/คู่มือให้แก่ธนาคารภายในเวลาที่ธนาคารกำหนดดังต่อไปนี้

6.1 คู่มือประจำเครื่อง (Manual) ของอุปกรณ์ทุกรายการที่เสนอในโครงการ ในลักษณะของแฟ้มงานจำนวน 1 แฟ้ม และจัดทำ Index ของเอกสาร แบ่งแยกเอกสารแต่ละชุดอย่างชัดเจนให้แก่ธนาคาร

6.2 คู่มือการการติดตั้งอุปกรณ์ทุกรายการในโครงการนี้และคู่มือการใช้งาน ในลักษณะของแฟ้มงานจำนวน 1 แฟ้ม และจัดทำ Index ของเอกสาร แบ่งแยกเอกสารแต่ละชุดอย่างชัดเจนให้แก่ธนาคาร

7. ลิขสิทธิ์ Software

ผู้ที่ได้รับการคัดเลือกที่ได้เป็นคู่สัญญากับธนาคาร จะต้องเป็นผู้รับผิดชอบให้ธนาคารมีสิทธิโดยถูกต้องอันชอบธรรมในการใช้ Software ที่เสนอและ/หรือ Software ที่จำเป็นต้องใช้ในระบบที่ได้ส่งมอบให้แก่ธนาคาร รวมถึงสิทธิ์การใช้งานสำหรับ Tool และ/หรือ Application ที่ใช้ในการดำเนินการในโครงการนี้ทั้งหมด จะต้องมอบให้เป็นของธนาคารอย่างถูกต้องตามกฎหมายจากเจ้าของลิขสิทธิ์ ในกรณีที่ผู้ที่ได้รับการคัดเลือกทำการแก้ไขและพัฒนาเพิ่มเติม Tool และ/หรือ Application นั้น (Customize & Development) ผู้ที่ได้รับการคัดเลือกต้องมอบให้เป็นลิขสิทธิ์ของธนาคารด้วย ทั้งการเป็นเจ้าของลิขสิทธิ์และการใช้งานซึ่งธนาคารสามารถดำเนินการอย่างไรก็ได้กับการแก้ไข และการพัฒนาเพิ่มเติม Tool และ/หรือ Application นั้น โดยผู้ที่ได้รับการคัดเลือกไม่สามารถเรียกร้องลิขสิทธิ์หรือเรียกร้องค่าใช้จ่ายเพิ่มเติมได้อีกในการกระทำกับ Tool และ/หรือ Application นั้น ๆ ทั้งที่มีลิขสิทธิ์อยู่แล้ว หรืออาจมีลิขสิทธิ์เกิดขึ้นภายหลัง

8. ความต้องการด้านความปลอดภัยสารสนเทศ

ผู้ได้รับการคัดเลือกต้องดำเนินการป้องกันด้านความปลอดภัยของระบบสารสนเทศที่เกี่ยวข้องทั้งหมด เช่น ระบบปฏิบัติการ ระบบฐานข้อมูล ระบบเครือข่าย เป็นต้น พร้อมแก้ไขประเด็นที่ตรวจพบให้แล้วเสร็จ ก่อนส่งมอบคู่มือ (Manual) และรายการ (Checklist) ให้แก่ธนาคารดังนี้

8.1 รายการทรัพย์สินสารสนเทศในระบบทั้งหมด พร้อมลิขสิทธิ์การใช้งาน (License)

8.2 ผลการติดตั้ง Software Patches ให้เป็นปัจจุบัน เพื่อลดหรือกำจัดข้อบกพร่องด้านความมั่นคงปลอดภัย

8.3 ผลการตั้งค่าความปลอดภัยขั้นต่ำของระบบ (IT Security Baseline) ตามที่ธนาคารกำหนดทั้งหมด โดยให้ติดตั้งและทดสอบระบบใน Development Environment ก่อนติดตั้งในระบบ Production

8.4 ผลการตรวจสอบช่องโหว่ (Vulnerability Assessment) ที่มีการแก้ไขเรียบร้อยแล้ว

8.5 ผลการทดสอบบุกรุกเจาะระบบ (Penetration Testing) ที่มีการแก้ไขเรียบร้อยแล้ว

8.6 ส่งมอบรายชื่อบัญชีผู้ใช้งานของระบบ เช่น Operating System Account หรือที่เกี่ยวข้อง

8.7 เอกสารการออกแบบระบบ (Design System Diagram) ให้ธนาคารพิจารณาความเหมาะสม

8.8 แผนการรับมือต่อเหตุการณ์ผิดปกติด้านการรักษาความมั่นคงปลอดภัย เช่น แผนรับมือภัยด้านไซเบอร์ เป็นต้น

ธนาคารอาคารสงเคราะห์ให้ความสำคัญกับการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ธนาคารจึงได้กำหนดนโยบายคุ้มครองข้อมูลส่วนบุคคล โดยสามารถศึกษารายละเอียดที่ QR Code นี้