แบบ บก.06

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย
การจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ จัดซื้อค่าลิขสิทธิ์ซอฟต์แวร์ Breach and Attack Simulation (BAS) เพื่อสำหรับการทดสอบบุกรุกระบบ (Penetration Testing)
2. หน่วยงานเจ้าของโครงการ ศูนย์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ธนาคารอาคารสงเคราะห์ สำนักงานใหญ่
3. วงเงินงบประมาณที่ได้รับจัดสรร 7,500,000.- บาท (เจ็ดล้านห้าแสนบาทถ้วน)
4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ 30 พ.ค. 2568
   เป็นเงิน 7,383,000.- บาท (เจ็ดล้านสามแสนแปดหมื่นสามพันบาทถ้วน) รวมภาษีมูลค่าเพิ่มแล้ว
5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
   5.1 สืบจากท้องตลาด จำนวน 3 บริษัท ได้แก่
   - บริษัท อินฟินิตี้ ทู อินฟินิตี้ จำกัด
   - บริษัท เอ็กซ์ฟินิท จำกัด
   - บริษัท ดาต้าฟาร์ม จำกัด
6. รายชื่อผู้รับผิดชอบในการกำหนดค่าใช้จ่าย/ดำเนินการ/ขอบเขตดำเนินการ (TOR)
   (ตามบันทึกข้อความที่ ศม.216/2567 ลว. 27 พ.ย.2567)

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

ขอบเขตงาน (Terms of Reference : TOR)
โครงการจัดซื้อค่าลิขสิทธิ์ซอฟต์แวร์ Breach and Attack Simulation (BAS) **เพื่อสำหรับ**
การทดสอบบุกรุกระบบ (Penetration Testing)
เลขที่ 102 - 91 / 2568

1. ความเป็นมา/เหตุผลและความจำเป็น

ความเจริญก้าวหน้าด้านเทคโนโลยีสารสนเทศและการสื่อสารในรูปแบบและเทคนิคใหม่ๆ เข้ามามีบทบาทมากขึ้นในขณะเดียวกันพบว่าปัญหาความไม่ปลอดภัยด้านเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามด้านไซเบอร์ที่เพิ่มมากขึ้นเช่นกัน และมีแนวโน้มที่จะขยายตัวเพิ่มขึ้นในทุกภาคส่วน ซึ่งอาจสร้างความเสียหายให้กับธนาคารได้อย่างมาก ดังนั้นธนาคารจึงมีความจำเป็นต้องจัดซื้อซอฟต์แวร์ สำหรับจำลองรูปแบบการโจมตีระบบสารสนเทศของธนาคาร ด้วยเทคนิคและรูปแบบใหม่ (Breach and Attack Simulation) ได้เป็นประจำอย่างต่อเนื่อง เพื่อใช้ในการศึกษา เทคนิค วิธีการ รูปแบบการโจมตี ผลกระทบการโจมตี และหามาตรการป้องกันระบบสารสนเทศของธนาคาร ก่อนเกิดเหตุการณ์จริง ซึ่งจะช่วยเพิ่มประสิทธิภาพการเฝ้าระวังการโจมตีทางไซเบอร์รูปแบบต่างๆ ที่เกิดขึ้น ที่อาจมีผลกระทบกับการดำเนินงานของระบบสารสนเทศของธนาคาร และการรั่วไหลของข้อมูลได้

2. วัตถุประสงค์

2.1 เพื่อให้ธนาคารสามารถ จำลองรูปแบบการโจมตีระบบสารสนเทศของธนาคาร ด้วยเทคนิค วิธีการ และรูปแบบใหม่ได้เป็นประจำอย่างต่อเนื่อง

2.2 เพื่อให้ธนาคารสามารถศึกษา เทคนิค วิธีการ ข้อมูลการโจมตีทางไซเบอร์ต่างๆ และนำมาใช้ในการวิเคราะห์ และปรับปรุงระบบป้องกันของธนาคารได้

2.3 เพื่อให้ธนาคารสามารถ ติดตาม เฝ้าระวัง และป้องกันภัยคุกคามทางไซเบอร์ต่างๆ ที่เกิดขึ้นในระบบงานของธนาคาร ทั้งในส่วนของระบบงานหลัก GHB System, ระบบงานที่ให้บริการ Electronic Channel และระบบงานสนับสนุนระบบสารสนเทศของธนาคาร

2.4 เพื่อให้ธนาคารสามารถบริหารจัดการภัยคุกคามทางไซเบอร์ต่างๆ ที่เกิดขึ้น ในระบบงานของธนาคารได้อย่างมีประสิทธิภาพ

3. คุณสมบัติของผู้เสนอราคา

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

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 ผู้ยื่นข้อเสนอต้องไม่เคยถูกยกเลิกสัญญาซื้อขาย หรือสัญญาจ้างบริการบำรุงรักษาฯ ก่อนหมดอายุสัญญา โดยไม่มีเหตุผลอันควรจากธนาคาร หรือหน่วยงานใดๆ

3.11 ผู้ยื่นข้อเสนอทุกรายจะต้องเก็บรักษาข้อมูลที่เกี่ยวข้องทั้งหมดของธนาคารไว้เป็นความลับ จะไปเผยแพร่ที่อื่นมิได้

3.12 ผู้ยื่นข้อเสนอต้องมีผู้เชี่ยวชาญในการเฝ้าระวังและวิเคราะห์ภัยคุกคาม โดยมีใบรับรอง (Certified) CompTIA CASP+ หรือ CYSA+ หรือ CISSP (Certified Information System Security Professional) หรือ OSCP (Offensive Security Certified Professional) อย่างใดอย่างหนึ่งหรือมากกว่า

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) ตารางเปรียบเทียบคุณลักษณะเฉพาะของซอฟต์แวร์ Breach and Attack Simulation (BAS) เพื่อสำหรับการทดสอบบุกรุกระบบ (Penetration Testing) ที่เสนอกับคุณลักษณะเฉพาะที่ธนาคารกำหนด

(3) หนังสือมอบอำนาจซึ่งปิดอากรแสตมป์ตามกฎหมายในกรณีที่ผู้ยื่นข้อเสนอราคามอบอำนาจ ให้บุคคลอื่นลงนามในใบเสนอราคาแทน

(4) บัญชีเอกสารส่วนที่ 2 ทั้งหมดที่ได้ยื่นพร้อมกับซองใบเสนอราคา

5. เอกสารประกอบการเสนอราคา

ผู้ยื่นข้อเสนอต้องนำเสนอสิทธิการใช้งานซอฟต์แวร์ Breach and Attack Simulation (BAS) เพื่อสำหรับการทดสอบบุกรุกระบบ (Penetration Testing) เป็นระยะเวลา 1 ปี โดยมีรายละเอียด เอกสารประกอบการเสนอราคา ดังนี้

5.1 ข้อมูลเกี่ยวกับประวัติ และความเป็นมาของบริษัทผู้ยื่นข้อเสนอ รวมถึงลักษณะการดำเนินงาน ผลประกอบการที่ผ่านมา 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 ในการจัดซื้อค่าลิขสิทธิ์ซอฟต์แวร์ Breach and Attack Simulation (BAS) เพื่อสำหรับ การทดสอบบุกรุกระบบ (Penetration Testing) ของธนาคาร ข้อเสนอของผู้ยื่นข้อเสนอรวมทั้งข้อเสนอเพิ่มเติมในการต่อรองให้ถือเป็นส่วนหนึ่ง ของสัญญาด้วย

รายละเอียดต่างๆ ที่ผู้ยื่นข้อเสนอเสนอมานั้น หากมีปัญหาในการตีความของข้อความใด ให้ถือคำวินิจฉัยของธนาคารเป็นที่ยุติ

6. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

การพิจารณาผู้ชนะการยื่นข้อเสนอ ธนาคารจะพิจารณาจากเกณฑ์ราคา และจะพิจารณาจากราคารวม

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

ผู้ยื่นข้อเสนอต้องนำเสนอซอฟต์แวร์ Breach and Attack Simulation (BAS) เพื่อสำหรับการทดสอบบุกรุกระบบ (Penetration Testing) พร้อมติดตั้ง โดยมีรายละเอียดของงาน ตามเอกสารแนบ

9. ระยะเวลาดำเนินการ

ระยะเวลาดำเนินการส่งมอบสิทธิการใช้งาน พร้อมติดตั้งซอฟต์แวร์ Breach and Attack Simulation (BAS) เพื่อสำหรับการทดสอบบุกรุกระบบ (Penetration Testing) ภายใน 60 วัน นับถัดจากวันที่ลงนามในสัญญา โดยมีเงื่อนไขตามเอกสารแนบ

10. วงเงินที่จะจัดซื้อจัดจ้าง

วงเงินงบประมาณ 7,500,000.- บาท (เจ็ดล้านห้าแสนบาทถ้วน)

11. เงื่อนไขการชำระเงิน

ธนาคารจะชำระเงินค่าจัดซื้อสิทธิการใช้งานซอฟต์แวร์ Breach and Attack Simulation (BAS) เพื่อสำหรับการทดสอบบุกรุกระบบ (Penetration Testing) หลังจากที่ได้ตรวจรับการส่งมอบงานถูกต้องครบถ้วนเรียบร้อยตามเงื่อนไขสัญญา ตามที่ธนาคารกำหนด โดยจะชำระเงิน แบ่งเป็น 2 งวด ตามเงื่อนไขดังนี้

งวดที่ 1 จำนวน 40% ของมูลค่าตามสัญญา (ภายในระยะเวลา 30 วัน นับถัดจากวันลงนามในสัญญา) เมื่อผู้ได้รับการคัดเลือกดำเนินการจัดส่งสิทธิการใช้งานซอฟต์แวร์ Breach and Attack Simulation (BAS) เพื่อสำหรับการทดสอบบุกรุกระบบ (Penetration Testing)เรียบร้อยแล้ว

งวดที่ 2 จำนวน 60% ของมูลค่าตามสัญญา (ภายในระยะเวลา 60 วัน นับถัดจากวันลงนามในสัญญา) เมื่อผู้ได้รับการคัดเลือกดำเนินการติดตั้งซอฟต์แวร์ Breach and Attack Simulation (BAS) เพื่อสำหรับการทดสอบบุกรุกระบบ (Penetration Testing) รวมถึงดำเนินการฝึกอบรม และคณะกรรมการตรวจรับได้ตรวจรับมอบแล้วเห็นว่าถูกต้องตรงตามเงื่อนไขของสัญญา

12. อัตราค่าปรับ

กำหนดค่าปรับเป็นรายวันในอัตราร้อยละ 0.20 ของราคาพัสดุที่ยังไม่ได้รับมอบ

13. ระยะเวลาการใช้งาน/สิทธิการใช้งาน

ผู้ได้รับการคัดเลือกต้องรับประกันให้ธนาคารสามารถซอฟต์แวร์ Breach and Attack Simulation (BAS) เพื่อสำหรับการทดสอบบุกรุกระบบ (Penetration Testing) ได้เป็นอย่างดีเป็นระยะเวลา 1 ปี นับถัดจากวันที่ธนาคารได้ตรวจรับมอบโดยถูกต้องครบถ้วนตามสัญญา โดยไม่คิดค่าใช้จ่ายใดๆ ทั้งสิ้น ในระหว่างระยะเวลาการรับประกันดังกล่าว

14. ข้อสงวนสิทธิ์ในการยื่นข้อเสนอและอื่น ๆ (ถ้ามี)

ธนาคารสงวนสิทธิ์ที่จะแก้ไขเพิ่มเติมเงื่อนไข หรือข้อกำหนดในแบบสัญญาหรือข้อตกลงซื้อเป็นหนังสือ ให้เป็นไปตามความเห็นของสำนักงานอัยการสูงสุด (ถ้ามี)

14.2 ในกรณีที่เอกสารแนบท้ายเอกสารการจัดซื้อ มีความขัดหรือแย้งกัน ผู้ยื่นข้อเสนอจะต้องปฏิบัติตามคำวินิจฉัยของธนาคาร คำวินิจฉัยดังกล่าวให้ถือเป็นที่สุด และผู้ยื่นข้อเสนอ ไม่มีสิทธิเรียกร้องค่าใช้จ่ายใด ๆ เพิ่มเติม

14.3 ธนาคารอาจประกาศยกเลิกการจัดซื้อในกรณีต่อไปนี้ได้ โดยที่ผู้ยื่นข้อเสนอจะเรียกร้องค่าเสียหาย ใด ๆ จากธนาคารไม่ได้

(1) ธนาคารไม่ได้รับการจัดสรรเงินที่จะใช้ในการจัดซื้อหรือที่ได้รับจัดสรรแต่ไม่เพียงพอ ที่จะทำการจัดซื้อครั้งนี้ต่อไป

(2) มีการกระทำที่เข้าลักษณะผู้ยื่นข้อเสนอที่ชนะการจัดซื้อหรือที่ได้รับการคัดเลือกมีผลประโยชน์ร่วมกัน หรือมีส่วนได้เสียกับผู้ยื่นข้อเสนอรายอื่น หรือขัดขวางการแข่งขัน อย่างเป็นธรรม 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

รายละเอียดและคุณลักษณะเฉพาะของ

โครงการจัดซื้อค่าลิขสิทธิ์ซอฟต์แวร์ Breach and Attack Simulation (BAS) เพื่อสำหรับการทดสอบบุกรุกระบบ (Penetration Testing)

คุณลักษณะเฉพาะของระบบงาน

โครงการจัดซื้อสิทธิการใช้งานซอฟต์แวร์ Breach and Attack Simulation (BAS) เพื่อสำหรับการทดสอบบุกรุกระบบ (Penetration Testing) ที่ธนาคารต้องการจัดหาเพื่อติดตั้งใช้งานที่ธนาคารอาคารสงเคราะห์ (สำนักงานใหญ่) ซึ่งมีรายละเอียด ดังนี้

1. **ซอฟต์แวร์ ที่นำเสนอต้องมีคุณลักษณะเฉพาะทางด้านเทคนิค ดังนี้**
    1. ต้องเป็นซอฟต์แวร์ออกแบบมาสำหรับจำลองภัยคุกคามโดยเฉพาะ โดยตัวบริหารจัดการ (Centralized Management) สามารถให้บริการในรูปแบบ Software as a Service (SaaS)
    2. ซอฟต์แวร์ที่นำเสนอ ต้องเป็นซอฟต์แวร์ที่อยู่ในกลุ่มของ Customer's Choice by Gartner Peer Insights ประจำปี 2024
    3. สามารถรองรับติดตั้ง Agent สำหรับทดสอบการโจมตีพร้อมกันได้ไม่น้อยกว่า 100 Agent หรือรองรับการติดตั้งแบบไม่จำกัดจำนวน โดยไม่มีค่าใช้จ่ายเพิ่มเติม
    4. สามารถติดตั้ง Agent สำหรับ จำลองการละเมิดและโจมตีบนระบบปฏิบัติการดังต่อไปนี้ได้เป็นอย่างน้อย
        - 4.1 Windows 10, 11
        - 4.2 Windows Server 2016, 2019, 2022
        - 4.3 Linux (Ubuntu, Debian, CentOS Redhat)
    5. มี Attack Module ในหมวดหมู่ดังต่อไปนี้เป็นอย่างน้อย
        - 5.1 Network Infiltration
        - 5.2 Email
        - 5.3 Web Application
        - 5.4 Endpoint
        - 5.5 Cloud WAF
        - 5.6 Data Exfiltration
        - 5.7 URL Filtering

6. สามารถจำลองการละเมิดและการโจมตีของภัยคุกคามที่เกิดขึ้นใหม่ เพื่อประเมินขีดความสามารถของการป้องกันที่ใช้อยู่ในปัจจุบันได้ โดยมีรายละเอียดดังนี้
    6.1 สามารถทดสอบภัยคุกคามที่เกิดขึ้นใหม่ ได้ผ่าน Web Gateway, Email Gateway และ Endpoint ได้เป็นอย่างน้อย
    6.2 สามารถสร้างภัยคุกคามใหม่ได้ โดยสามารถระบุ URL, IP และ Domain เพื่อทดสอบได้
    6.3 สามารถสร้างภัยคุกคามใหม่ ได้โดยสามารถ Upload Malicious file และ URL เพื่อทดสอบได้
    6.4 สามารถตั้งให้ทำการทดสอบภัยคุกคามที่เกิดขึ้นใหม่ได้โดยอัตโนมัติ
7. สามารถจำลองการละเมิดและการโจมตีผ่านช่องทาง Email เพื่อประเมินขีดความสามารถในการป้องกันภัยคุกคามของ Email Gateway ที่ใช้อยู่ในปัจจุบันได้ โดยมีรายละเอียดดังนี้
    7.1 ส่งไฟล์แนบ Malware ที่มีการทำงานตามเทคนิคดังนี้
        7.1.1 Escalate Privilege
        7.1.2 Collect credentials
        7.1.3 Communicate with C2 via emails
    7.2 ส่งไฟล์แนบเอกสาร Microsoft Office ที่มีพฤติกรรมที่เป็นอันตราย และ ช่องโหว่ (known vulnerabilities) เช่น doc, docx, pptx, xlsx ได้เป็นอย่างน้อย
    7.3 รวบรวมและส่ง Link ที่ถูกระบุว่าเป็นอันตรายจาก CERTS หรือ Threat intelligence engines เข้ามาตรวจสอบ
8. สามารถจำลองการละเมิดและการโจมตี ผ่านช่องทางการใช้งานผ่าน Protocol HTTP และ HTTPS เพื่อประเมินขีดความสามารถในการป้องกันภัยคุกคามของ Web Gateway ที่ใช้อยู่ในปัจจุบันได้ โดยมีรายละเอียดดังนี้
    8.1 สามารถทดสอบการดาวน์โหลด Malware, Exploits, Ransomware, Worm, Payloads ได้เป็นอย่างน้อย
    8.2 สามารถทดสอบการเข้าถึงเว็บไซต์ที่จัดอยู่ในประเภทอันตรายเช่น Phishing และ C&C ได้เป็นอย่างน้อย
    8.3 สามารถทดสอบการดาวน์โหลด Real Malware และมีการควบคุมโดยไม่ให้มีการทำงานของ malware บนเครื่องที่ดาวน์โหลด
    8.4 สามารถจำลองการทำงาน Tactics และ Techniques ของ Malware ได้
    8.5 สามารถทดสอบนโยบายเกตเวย์ของเว็บเพื่อทดสอบไปยังเว็บไซต์ต้องห้าม เช่น Gambling, Adult ได้เป็นอย่างน้อย

9. มีประเภทของ Attack ให้เลือกใช้มากกว่า 900 Threats หรือ มี Action ในการโจมตีไม่น้อยกว่า 20,000 Actions รวมถึงต้องมีการ update ฐานข้อมูลอย่างต่อเนื่อง
10. มี Dashboard ที่สามารถแสดงประสิทธิภาพในการป้องกันและประสิทธิภาพในการตรวจจับ Threat โดยรวม โดยสามารถแสดงข้อมูลย้อนหลังได้
11. สามารถแสดงข้อมูลประสิทธิภาพในการป้องกันได้ โดยสามารถแสดงจำนวน event หรือ actions ดังต่อไปนี้
    11.1 จำนวนครั้งที่สามารถ block ได้ และไม่สามารถ block ได้
    11.2 แสดงค่าร้อยละ (%) ประสิทธิภาพในการป้องกันบนอุปกรณ์
    11.3 แสดงกราฟข้อมูลย้อนหลัง ประสิทธิภาพในการป้องกันบนอุปกรณ์
12. สามารถแสดงข้อมูลประสิทธิภาพในการตรวจจับโดยสามารถแสดงจำนวน event หรือ actions ดังต่อไปนี้ได้
    12.1 จำนวนครั้งที่สามารถ log ได้ และไม่สามารถ log ได้
    12.2 จำนวนครั้งที่สามารถ alert ได้ และไม่สามารถ alert ได้
    12.3 แสดงค่าร้อยละ (%) ประสิทธิภาพในการตรวจจับบนอุปกรณ์
    12.4 แสดงกราฟข้อมูลย้อนหลัง ประสิทธิภาพในการตรวจจับบนอุปกรณ์
13. สามารถ validate ข้อมูล log และ alert บนผลิตภัณฑ์ SIEM ที่ธนาคารใช้งานอยู่ได้ (Splunk)
14. สามารถแสดงข้อมูลผลการทดสอบเข้ากับ MITRE ATT&CK Framework ได้
15. สามารถจำลองการละเมิดและโจมตีที่เกิดขึ้นกับอุปกรณ์ Endpoint เพื่อประเมินขีดความสามารถในการป้องกันภัยคุกคามของ Endpoint Security ที่ใช้อยู่ในปัจจุบัน โดยมีรายละเอียดดังนี้
    15.1 สามารถจำลองการทำงานตาม Tactics และ Techniques ที่เป็น Behavior-based ของ Ransomware, Worm , Rootkit และ Trojan ได้เป็นอย่างน้อย
    15.2 หลังจากทำการทดสอบแล้ว สามารถแนะนำแนวทางการสร้าง Rules สำหรับ SIEM ที่ธนาคารใช้งานอยู่ (Splunk) ได้
16. ซอฟต์แวร์ที่นำเสนอต้องได้รับการจัดอันดับให้เป็น Leader ในรายงาน Frost & Sullivan Breach and Attack Simulation ปี ค.ศ. 2022 หรือล่าสุด
17. สามารถแสดงข้อมูลการแนะนำโดยเฉพาะเจาะจง หรือ Specific Mitigation สำหรับแต่ละ Vendor เพื่อให้สามารถนำไปปรับปรุงประสิทธิภาพการรักษาความปลอดภัยขององค์กรได้
18. สามารถทดสอบแบบ Manual หรือตั้ง Schedule ในการทดสอบได้ รวมถึงสามารถสร้างการทดสอบแบบ custom threat ได้อย่างอิสระ

19. มี Threat Template ให้สามารถเลือกใช้ทดสอบได้ทั้งในรูปแบบ Static และ Dynamic รวมถึงสามารถสร้าง Threat Template ขึ้นมาใช้งานเองได้ทั้งแบบ Static และ Dynamic ตามเงื่อนไขที่กำหนด
20. สามารถจัดเตรียมกฎการตรวจจับที่เขียนในรูปแบบไวยากรณ์ของบนผลิตภัณฑ์ SIEM ที่ธนาคารใช้งานอยู่ (Splunk) เพื่อให้ง่ายต่อการแก้ไขกฎการตรวจจับ (Detection Rules) บน SIEM ได้
21. สามารถทำ Lateral Movement, การเก็บข้อมูล และ Credentials เพื่อนำมาทดสอบภายในระบบ
22. สามารถจำลองการโจมตีเต็มรูปแบบ (Full Kill Chain Scenarios หรือ Attack Scenarios) โดยอ้างอิงหรือจำลองจาก real-world APTs เช่น Lazarus Group ได้เป็นอย่างน้อย
23. สามารถสร้างการโจมตีแบบเต็มรูปแบบ (Full Kill Chain Scenarios หรือ Attack Scenarios) ขึ้นมาเพื่อทดสอบได้ เช่น กำหนด Malicious Code, Vulnerabilities Exploitation, Process ได้เป็นอย่างน้อย
24. ซอฟต์แวร์ที่นำเสนอจะต้องมีเซิร์ฟเวอร์ C2 ที่ใช้ในการตัดสินใจว่าขั้นตอนหรือการดำเนินการใดที่จะดำเนินการโดยใช้ข้อมูลที่รวบรวมจาก Endpoint หรือ Domain
25. ซอฟต์แวร์ที่นำเสนอจะต้องดำเนินการจำลองการถอดรหัสรหัสผ่านภายในสภาพแวดล้อมเฉพาะที่จัดการโดยผู้จำหน่าย เพื่อให้มั่นใจว่ากิจกรรมเหล่านี้จะไม่นำไปใช้หรือส่งผลกระทบต่อทรัพยากร–หรือประสิทธิภาพของระบบของลูกค้า
26. ซอฟต์แวร์ที่นำเสนอจะต้องสามารถค้นพบจุดอ่อนใน AD และระบบปฏิบัติการได้
27. ความเสี่ยงที่ค้นพบจะต้องรวมถึงความรุนแรง, สาเหตุที่แท้จริง, ผลกระทบ, หมวดหมู่, ผู้ขาย, ผลิตภัณฑ์, การแมปเทคนิค MITER ATT&CK, คำอธิบาย, และคำแนะนำในการบรรเทาผลกระทบ
28. สามารถจำลองและทดสอบการ Lateral Movement ไปยังเครื่องที่ไม่ได้ติดตั้ง Agent ได้เพื่อประเมินการแพร่กระจายภายในเครือข่ายและเข้าควบคุมระบบได้ดังนี้
    - 28.1 สามารถกำหนด Attack Actions ได้ เช่น Discovery, Credentials Access, Privilege Escalation และ Impact ได้เป็นอย่างน้อย-พร้อมทั้งสามารถเลือก ชนิดไฟล์ที่จะทำการทดสอบได้ เช่น .doc, .xls, .ppt และ .pdf ได้เป็นอย่างน้อย
    - 28.2 สามารถกำหนดวิธีการในการจำลอง Lateral Movement ได้เช่น SMB, Pass the Hash และ Pass the Ticket ได้เป็นอย่างน้อย
    - 28.3 สามารถกำหนด Scope ในการทดสอบ และ Scope ที่ไม่ต้องการให้ทดสอบได้
    - 28.4 สามารถแสดงการแพร่กระจายโดยอยู่ในรูปแบบแผนภาพ และรายละเอียดของการแพร่กระจายได้

2. เงื่อนไขการติดตั้งและส่งมอบ

2.1 ผู้ที่ได้รับการผู้ที่ได้รับการคัดเลือกต้องจัดส่งสิทธิการใช้งานซอฟต์แวร์ Breach and Attack Simulation (BAS) เพื่อสำหรับการทดสอบบุกรุกระบบ (Penetration Testing) ที่ซื้อขาย ณ ธนาคารอาคารสงเคราะห์ สำนักงานใหญ่ ให้ครบถ้วนภายใน 30 วัน นับถัดจากวันที่ลงนามในสัญญา

2.2 ผู้ที่ได้รับการคัดเลือกจะต้องดำเนินการติดตั้งซอฟต์แวร์ Breach and Attack Simulation (BAS) เพื่อสำหรับการทดสอบบุกรุกระบบ (Penetration Testing) ที่ซื้อขาย ณ ธนาคารอาคารสงเคราะห์ สำนักงานใหญ่ ให้ครบถ้วนภายใน 60 วัน นับถัดจากวันที่ลงนามในสัญญา

2.3 ผู้ที่ได้รับการคัดเลือกจะต้องจัดส่งเอกสาร คู่มือฉบับภาษาไทย หรือ Media คู่มือการปฏิบัติงานของ ซอฟต์แวร์ Breach and Attack Simulation (BAS) เพื่อสำหรับการทดสอบบุกรุกระบบ (Penetration Testing) 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 30 วัน) ภายในระยะเวลา 1 ปี (นับถัดจากวันที่ลงนามในสัญญา) โดยธนาคารจะเป็นผู้กำหนดวันเข้ามาปฏิบัติงานที่ธนาคาร เพื่อให้คำปรึกษาและดำเนินการปรับแต่งเพิ่มเติมและแก้ไขค่าคอนฟิกซอฟต์แวร์ เพื่อให้สามารถทำงานได้อย่างมีประสิทธิภาพ

2.5 ผู้ที่ได้รับการคัดเลือกจะต้องจัดหลักสูตรการฝึกอบรมให้แก่ผู้ดูแลระบบ หัวข้อ การใช้งานและการดูแล ซอฟต์แวร์ Breach and Attack Simulation (BAS) เพื่อสำหรับการทดสอบบุกรุกระบบ (Penetration Testing) ให้ครบถ้วนภายใน 60 วัน นับถัดจากวันที่ลงนามในสัญญา

2.6 ผู้ที่ได้รับการคัดเลือกต้องดำเนินการส่งมอบเครื่องคอมพิวเตอร์พกพา (Notebook) จำนวน 1 เครื่อง ที่มีการติดตั้ง Agent ของระบบที่นำเสนอเพื่อช่วยให้สามารถนำเครื่องคอมพิวเตอร์พกพา (Notebook) ดังกล่าวไปใช้ทดสอบจำลองการโจมตีระบบสารสนเทศของธนาคาร ตามเครือข่ายที่ต้องการได้ โดยมีคุณสมบัติขั้นต่ำ ดังนี้

2.6.1 มีหน่วยประมวลผลกลาง (CPU) Intel Core Ultra 5 หรือดีกว่า

2.6.2 มีหน่วยความจำหลัก (RAM) ชนิด DDR5 หรือดีกว่า และมีขนาดความจุไม่น้อยกว่า 32 GB

2.6.3 มีหน่วยจัดเก็บข้อมูล (Hard Disk) ชนิด Solid State Drive ขนาดความจุไม่น้อยกว่า 500 GB

2.6.4 มีระบบปฏิบัติการ Windows 11 Pro (64 bit)

2.6.5 มีขนาดหน้าจอ 13.3 – 15 นิ้ว

3. การฝึกอบรม

ผู้ที่ได้รับการคัดเลือกต้องจัดการฝึกอบรมให้แก่ผู้เข้าฝึกอบรมของธนาคารภายในเวลา 60 วัน นับถัดจากวันลงนามในสัญญาซึ่งมีหัวข้อของหลักสูตรที่ครอบคลุมทั้งภาคทฤษฎีและภาคปฏิบัติอย่างน้อย ดังนี้

ที่	ชื่อหลักสูตร	จำนวนวัน	สถานที่อบรม	จำนวนครั้ง	จำนวนคนต่อครั้ง
1	การใช้งานและการดูแลซอฟต์แวร์ Breach and Attack Simulation (BAS) เพื่อสำหรับการทดสอบบุกรุกระบบ (Penetration Testing)	2	ธนาคารอาคารสงเคราะห์ (สำนักงานใหญ่) หรือตามที่ธนาคารกำหนด	1	5

ทั้งนี้ การฝึกอบรมทุกครั้ง ผู้ที่ได้รับการคัดเลือกจะต้องเป็นผู้ดำเนินการจัดหาติดตั้งอุปกรณ์ที่เกี่ยวข้องที่ต้องใช้ในการฝึกอบรม พร้อมทั้งสนับสนุนเอกสารและวัสดุที่ใช้ในการฝึกอบรมให้กับผู้เข้าฝึกอบรม พร้อมทั้งบริการกาแฟ และอาหารว่าง โดยต้องจัดเตรียมให้เพียงพอต่อผู้เข้าฝึกอบรม โดยไม่มีค่าใช้จ่ายใด ๆ ทั้งสิ้น

4. ลิขสิทธิ์ Software

ผู้ที่ได้รับการคัดเลือกที่ได้เป็นคู่สัญญากับธนาคาร จะต้องเป็นผู้รับผิดชอบให้ธนาคารมีสิทธิโดยถูกต้องอันชอบธรรมในการใช้ซอฟต์แวร์ ที่เสนอและ/หรือ ซอฟต์แวร์ 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

ธนาคารอาคารสงเคราะห์ให้ความสำคัญกับการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ธนาคารจึงได้กำหนดนโยบายคุ้มครองข้อมูลส่วนบุคคล โดยสามารถศึกษารายละเอียดที่ QR Code นี้