กทท. การท่าเรือแห่งประเทศไทย

ขอบเขตของงาน (Terms of Reference : TOR)
เช่าใช้ระบบตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์ของระบบเครื่องคอมพิวเตอร์แม่ข่าย

การท่าเรือแห่งประเทศไทย (กทท.) ประสงค์จะเช่าใช้ระบบตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์ของระบบเครื่องคอมพิวเตอร์แม่ข่าย ปีงบประมาณ 2568 เป็นการเช่าใช้ระบบป้องกันภัยคุกคามทางไซเบอร์เพื่อให้สามารถตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์ก่อนที่จะก่อให้เกิดความเสียหายของข้อมูล หรือระบบปฏิบัติการ แก่เครื่องคอมพิวเตอร์แม่ข่ายที่ กทท. ใช้งานอยู่ในปัจจุบัน โดยได้กำหนดเงื่อนไขและขอบเขตการดำเนินงานไว้ ดังนี้

1. ความเป็นมา

ระบบตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์ดังกล่าวมีหน้าที่ในการป้องกัน วิเคราะห์เหตุการณ์ ตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ให้กับระบบเครื่องคอมพิวเตอร์แม่ข่ายได้แบบอัตโนมัติ เพื่อให้ระบบงานสารสนเทศทั้งหมดของ กทท. มีความปลอดภัยต่อภัยคุกคามทางไซเบอร์ และสามารถให้บริการได้อย่างต่อเนื่อง ทั้งนี้ หากเกิดเหตุภัยคุกคามทางไซเบอร์ ทำให้ส่วนใดส่วนหนึ่งของเครื่องคอมพิวเตอร์แม่ข่ายเกิดความเสียหาย อาจเป็นเหตุให้ไม่สามารถให้บริการได้ ซึ่งจะก่อให้เกิดผลกระทบต่อการให้บริการของ กทท. จึงจำเป็นต้องทำการเช่าใช้ระบบตรวจสอบดังกล่าว เพื่อให้เครื่องคอมพิวเตอร์แม่ข่ายสามารถใช้งานได้ตามปกติ

2. วัตถุประสงค์

2.1 เพื่อเช่าใช้ระบบตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์ของระบบเครื่องคอมพิวเตอร์แม่ข่าย ให้สามารถตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์ได้ตลอด 24 ชั่วโมง

2.2 เพื่อเพิ่มประสิทธิภาพในการป้องกัน ค้นหา และวิเคราะห์ภัยคุกคามใหม่ ๆ ที่จะเกิดขึ้นในอนาคตกับระบบสารสนเทศของระบบเครื่องคอมพิวเตอร์แม่ข่ายของ กทท. ได้อย่างมีประสิทธิภาพและทันท่วงที

3. คุณสมบัติเฉพาะของผู้เสนอราคา

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลางซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพรับจ้างงานดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ กทท. ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสารสิทธิ์หรือความคุ้มกันซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่ รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

1. ..... 2. ..... 3. ..... 4. ..... 5. .....

3.10 ผู้ยื่นข้อเสนอที่ยื่นเสนอราคาในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติ ดังนี้

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลักกิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลักผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน หรือหนังสือเชิญชวน

3.11 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ มูลค่าการจัดซื้อจัดจ้างเกิน 1 ล้านบาท แต่ไม่เกิน 5 ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า 1 ล้านบาท

(3) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน 500,000 บาทขึ้นไปกรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา ให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน 90 วัน ก่อนวันยื่นข้อเสนอโดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้งและหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

(4) กรณีผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียนหรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดนต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอนับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน)

3.12 ข้อยกเว้น กรณีตามข้อ 3.11 ไม่ใช้บังคับกรณีดังต่อไปนี้

(1) ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(2) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ 10) พ.ศ. 2561

3.13 มีผลงานที่เกี่ยวข้องกับระบบตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานราชการ รัฐวิสาหกิจ หรือเอกชนที่ กทท. เชื่อถือได้ โดยมีมูลค่างานรวมภาษีมูลค่าเพิ่ม ไม่น้อยกว่า 1 (หนึ่ง) ล้านบาท โดยผลงานดังกล่าวต้องมีอายุไม่เกิน 5 ปี นับจนถึงวันยื่นเอกสารเสนอราคา

3.14 ต้องได้รับการแต่งตั้งจากเจ้าของผลิตภัณฑ์ หรือสาขาเจ้าของผลิตภัณฑ์ ในประเทศไทย หรือตัวแทนจำหน่าย โดยให้ยื่นขณะเข้าเสนอราคา

3.15 ผู้ยื่นข้อเสนอต้องมีผู้เชี่ยวชาญและเจ้าหน้าที่ (พนักงานประจำ) ที่มีประสบการณ์และได้รับหนังสือรับรอง (Certificate) หลักสูตร CompTIA CySA+ หรือ CompTIA CASP+ หรือสูงกว่า

3.16 ผู้ยื่นข้อเสนอต้องมีผู้เชี่ยวชาญและเจ้าหน้าที่ (พนักงานประจำ) ที่มีประสบการณ์และได้รับใบประกาศนียบัตรของผลิตภัณฑ์ที่นำเสนอ

4. หลักฐานการยื่นข้อเสนอ

4.1 สำเนาหนังสือรับรองผลงาน หรือสำเนาสัญญาของงาน หรือสำเนาใบสั่งจ้างพร้อมขอบเขตของงาน (TOR) ตามข้อกำหนดข้อ 3.13 พร้อมรับรองสำเนาถูกต้อง โดยผู้ลงนามในหนังสือรับรองผลงานจะต้องได้รับมอบอำนาจจากหน่วยงานนั้นหรือเป็นผู้บริหารที่ กทท. เชื่อถือได้

4.2 สำเนาหนังสือแต่งตั้งตามข้อ 3.14 พร้อมรับรองสำเนาถูกต้อง

4.3 สำเนาเอกสารหนังสือรับรอง (Certificate) ตามข้อ 3.15 และหลักฐานการเป็นพนักงานประจำของบริษัทผู้เสนอราคา พร้อมรับรองสำเนาถูกต้อง

4.4 สำเนาเอกสารใบประกาศนียบัตร ตามข้อ 3.16 และหลักฐานการเป็นพนักงานประจำของบริษัทผู้เสนอราคา พร้อมรับรองสำเนาถูกต้อง

4.5 แคตตาล็อกและ/หรือแบบรูปรายการละเอียดคุณลักษณะเฉพาะ ตามภาคผนวก ก.

5. ระยะเวลาดำเนินการ

ผู้ให้เช่าจะต้องดำเนินการติดตั้งและปรับตั้งค่าระบบดังกล่าว ตามขอบเขตของงานข้อ 7.1 - 7.3 ให้แล้วเสร็จภายใน 45 วัน นับถัดจากวันลงนามในสัญญา

6. กำหนดเวลาส่งมอบพัสดุ

กำหนดระยะเวลาการเช่า 12 เดือน นับถัดจากวันที่คณะกรรมการตรวจรับพัสดุได้ให้ความเห็นชอบการติดตั้งและปรับตั้งค่าระบบฯ เรียบร้อยแล้ว

7. ขอบเขตของงาน

ผู้ให้เช่าจะต้องทำการจัดหาพร้อมติดตั้งระบบที่เสนอตามขอบเขตของงานให้สามารถทำงานได้อย่างมีประสิทธิภาพ ทั้งนี้ต้องเป็นผู้รับผิดชอบในการจัดหาวัสดุ เครื่องมือ เครื่องคอมพิวเตอร์ ซอฟต์แวร์ หรือ อุปกรณ์อื่น ๆ รวมถึงรับผิดชอบต่อค่าใช้จ่ายต่าง ๆ กรณีที่จำเป็นเพื่อให้สามารถดำเนินงานได้ตามขอบเขตของงานทั้งหมดที่ กทท. กำหนด กรณีที่มีข้อขัดแย้ง ข้อสงสัย หรือข้อผิดพลาดเกี่ยวกับสถานที่ติดตั้งและข้อกำหนดให้สอบถามต่อคณะกรรมการตรวจรับพัสดุ โดยตรงและการตีความในข้อขัดแย้งใด ๆ ให้ตีความไปในแนวทางที่วัสดุ ซอฟต์แวร์ หรืออุปกรณ์ที่มีคุณภาพที่ดีกว่าหรือมีจำนวนครบถ้วนกว่าทั้งสิ้น โดยต้องดำเนินการอย่างน้อยดังนี้

7.1 ความต้องการทั่วไป

7.1.1 คู่สัญญาต้องจัดทำแผนการทำงานมาให้ภายใน 15 วัน นับถัดจากวันลงนามในสัญญา

7.1.2 ระบบตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์ของระบบเครื่องคอมพิวเตอร์แม่ข่ายต้องมีลิขสิทธิ์การใช้งานที่ถูกต้องตามกฎหมาย จำนวนไม่น้อยกว่า 200 ลิขสิทธิ์ โดยสามารถใช้งานบนระบบปฏิบัติการตาม ภาคผนวก ข. ได้

7.2 เงื่อนไขในการติดตั้งและปรับตั้งค่า

7.2.1 ออกแบบและติดตั้งระบบที่มีคุณลักษณะเฉพาะตาม ภาคผนวก ก.

1. ..... 2. ..... 3. ..... 4. ..... 5. .....

7.2.2 ผู้ให้เช่าต้องติดตั้ง Agent บนเครื่องคอมพิวเตอร์แม่ข่าย ตามที่ กทท. กำหนด และตั้งค่าต่าง ๆ ให้สามารถทำงานได้ตรงตามวัตถุประสงค์ของขอบเขตของงาน โดยไม่ส่งผลกระทบต่อการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายที่ถูกติดตั้งรวมถึงมีการตั้งค่า เพื่อรวบรวมเหตุการณ์ความเสี่ยงจากระบบฯ ให้อยู่ในหน้าจอ (Dashboard) เดียวกันได้ พร้อมคู่มือการตั้งค่าและการใช้งานระบบฯ

7.2.3 ทำการทดสอบการป้องกันช่องโหว่ของระบบปฏิบัติการทางเครือข่ายได้บน Windows และ Linux ตามที่ กทท. กำหนด โดยที่ไม่จำเป็นต้องทำการติดตั้ง Patches หรือซอฟต์แวร์ใด ๆ บนระบบปฏิบัติการของ กทท.

7.2.4 ทำการทดสอบการป้องกันการโจมตีในระดับ Application Layer อาทิเช่น SQL injection และ Cross-Site Script และสามารถทำ SSL Inspection ได้ หรืออุปกรณ์เพิ่มเติม ตามที่ กทท. กำหนด

7.2.5 ติดตั้งและปรับตั้งค่าการแจ้งเตือนสถานะ (Alert Notification) ผ่าน Social Network (LINE Application) ได้ตามรูปแบบที่ทาง กทท. กำหนด

7.2.6 ติดตั้งและปรับตั้งค่าระบบเชื่อมต่อระหว่าง Security Agent และ Cloud เพื่อควบคุมการเข้าถึง Cloud Platform ของเจ้าของผลิตภัณฑ์

7.2.7 ติดตั้งและปรับตั้งค่าระบบให้สามารถส่ง Syslog จากระบบตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์ของระบบเครื่องคอมพิวเตอร์แม่ข่าย ไปยังเครื่องคอมพิวเตอร์แม่ข่าย ที่ กทท. กำหนด

7.2.8 หลังดำเนินการติดตั้งระบบฯ แล้วเสร็จ ผู้ให้เช่าต้องส่งหนังสือแจ้งคณะกรรมการตรวจรับพัสดุเพื่อพิจารณาว่าระบบฯ ติดตั้งแล้วเสร็จและพร้อมใช้งาน

7.3 เงื่อนไขการฝึกอบรม

ผู้ชนะการประกวดราคาฯ ต้องดำเนินการฝึกอบรมให้พนักงาน กทท. จำนวนไม่น้อยกว่า 3 คน ให้มีความรู้และความเข้าใจจนสามารถใช้ระบบฯ ได้อย่างมีประสิทธิภาพ โดยค่าใช้จ่ายที่เกิดขึ้นจากการฝึกอบรมเป็นค่าใช้จ่ายของผู้ชนะการประกวดราคาฯ ทั้งสิ้น ทั้งนี้การฝึกอบรมต้องดำเนินการโดยเจ้าของผลิตภัณฑ์หรือผู้ที่ได้รับการรับรองจากเจ้าของผลิตภัณฑ์ โดยการฝึกอบรมต้องมีหลักสูตรอย่างน้อยดังต่อไปนี้

- ด้านผู้ดูแลระบบตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์
- ด้านการตรวจสอบเฝ้าระวัง (Monitoring)
- ด้านการติดตั้ง Agent บนเครื่องคอมพิวเตอร์แม่ข่าย
- ด้านการแก้ไขปัญหา (Troubleshooting)

7.4 เงื่อนไขการดำเนินงาน

7.4.1 ให้คำแนะนำ และช่วยแก้ไขปัญหาต่าง ๆ เกี่ยวกับการใช้งานระบบฯ และภัยคุกคามทางไซเบอร์ที่ระบบฯ ตรวจจับได้

7.4.2 ทำการทดสอบการสแกนเครื่องคอมพิวเตอร์แม่ข่ายเพื่อหา Vulnerable Software แล้วจัดหาการตั้งค่า Recommended Security ที่เหมาะสมให้ หรือนำเข้าผลของการทำ Vulnerability Scan มาทำนโยบายความปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่อง จำนวนไม่ต่ำกว่า 100 เครื่อง และทำการปรับแต่งนโยบายความปลอดภัยการป้องกันช่องโหว่ของระบบปฏิบัติการทางเครือข่ายทั้งหมดแต่ละเครื่อง อย่างน้อยเดือนละ 1 ครั้ง

7.4.3 ทำการตรวจสอบการตั้งค่าของระบบป้องกันที่ติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่าย และระบบตรวจจับการโจมตีและตอบสนองภัยคุกคามโดยเจ้าของผลิตภัณฑ์ อย่างน้อยปีละ 1 ครั้ง

7.4.4 ประชุมกับ กทท. เดือนละ 1 ครั้ง หรือตามที่ กทท. ร้องขอ เพื่อสรุปภาพรวมผลการเฝ้าระวังภัยคุกคามและ ภัยคุกคามใหม่ที่เกิดขึ้น พร้อมให้คำปรึกษาในการรับมือกับภัยคุกคามที่อาจจะเกิดขึ้นให้ทางเจ้าหน้าที่ กทท. รับทราบ

7.4.5 กรณีที่เจ้าของผลิตภัณฑ์มีการปรับปรุงระบบฯ เป็นเวอร์ชั่นใหม่ ผู้ให้เช่าต้องแจ้งให้ผู้เช่าทราบเป็นลายลักษณ์อักษร และจะต้องทำการปรับปรุงระบบฯ เป็นเวอร์ชั่นใหม่ ในกรณีที่ กทท. ร้องขอ

7.4.6 ต้องให้ความร่วมมือกับ กทท. ในการปรับตั้งค่าให้สอดคล้องมาตรฐานต่าง ๆ หรือผลการตรวจสอบของผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอกที่เกี่ยวข้องตามที่ กทท. ร้องขอ โดยไม่คิดค่าใช้จ่ายเพิ่มเติม

8. ข้อกำหนดการดำเนินงาน

ผู้ให้เช่าจะต้องมีศูนย์รับแจ้ง (Call Center) สายด่วน (Hot Line) และ e-mail หรือ Line เพื่อเป็นช่องทางให้ กทท. แจ้งและติดต่อส่งรายละเอียดของปัญหาให้ผู้ให้เช่าได้ตลอด 24 ชั่วโมง

9. การส่งมอบงาน

9.1 ผู้ให้เช่าต้องจัดทำแผนการทำงาน ตามข้อ 7.1.1

9.2 ผู้ให้เช่าต้องส่งมอบเอกสารแสดงสิทธิ์การใช้งานของระบบตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์ตามข้อ 7.1.2 ภายใน 60 วันนับถัดจากวันลงนามในสัญญา

9.3 ผู้ให้เช่าต้องส่งมอบเอกสารการออกแบบและติดตั้งระบบ ตามข้อ 7.2.1

9.4 ผู้ให้เช่าต้องส่งมอบคู่มือการตั้งค่าและการใช้งานระบบฯ ตามข้อ 7.2.2

9.5 ผู้ให้เช่าต้องจัดทำรายงานสรุปผลการปฏิบัติงานประจำเดือน ในรูปแบบซอฟต์ไฟล์ จำนวน 1 ชุด ดังนี้

- รายงานการทดสอบการสแกนหา Vulnerable Software ตามข้อ 7.4.2
- รายงานการตรวจสอบการตั้งค่าของระบบป้องกันที่ติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่าย ตามข้อ 7.4.3 (ถ้ามี)
- รายงานสรุปผลการตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์ แบบรายเดือน (Monthly Report) ตามข้อ 7.4.4
- รายงานสรุปการแก้ไขปัญหากรณีเกิดข้อขัดข้องของระบบฯ หรือ กรณีที่เครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถใช้งานได้ตามปกติ ประกอบด้วย วัน/เวลาที่ กทท.อนุญาตให้เข้าดำเนินการแก้ไขปัญหา ชื่อผู้แจ้งปัญหา หน่วยงาน ปัญหาที่แจ้ง การแก้ไขปัญหา และวัน/เวลาที่แก้ไขปัญหาแล้วเสร็จ เป็นอย่างน้อย (ถ้ามี)

10. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

ผู้เสนอราคาต้องกรอกราคาในเอกสารรายละเอียดการเสนอราคาให้ครบถ้วน โดยราคารวมต้องตรงกับใบเสนอราคา ทั้งนี้ กทท. จะพิจารณาด้วยราคารวมต่ำสุด

11. งวดงานและการจ่ายเงิน

กำหนดงวดงานแบ่งเป็น 12 งวด โดย กทท. จะชำระค่าจ้างเป็นรายเดือน ตามระเบียบวิธีปฏิบัติในการจ่ายเงินของ กทท.

12. การเสนอราคา

ผู้เสนอราคาต้องปฏิบัติ ดังนี้

12.1 ราคาที่เสนอจะต้องเป็นราคาที่รวมภาษีมูลค่าเพิ่ม และภาษีอื่น ๆ (ถ้ามี) รวมค่าใช้จ่ายทั้งปวงไว้ด้วยแล้ว

12.2 ห้ามผู้เสนอราคาถอนการเสนอราคา

12.3 กทท. ขอสงวนสิทธิ์ที่จะลงนามในสัญญาจ้างต่อเมื่อได้รับอนุมัติงบประมาณแล้วเท่านั้น

12.4 กำหนดการยืนราคาไม่น้อยว่า 60 วัน นับแต่วันที่ยืนยันราคาสุดท้ายโดยภายในกำหนดยืนราคาห้ามผู้เสนอราคาถอนการเสนอราคา

12.5 คู่สัญญาต้องจัดทำแผนการทำงานมาให้ภายใน 15 วัน นับถัดจากวันลงนามในสัญญา โดยจัดทำแผนการทำงานตามเอกสารแนบ เว้นแต่เป็นกรณีการเช่า สัญญาอายุไม่เกิน 90 วัน หรือสัญญาที่มีวงเงินไม่เกิน 500,000 บาท ทั้งนี้ แผนการทำงานดังกล่าวให้ถือเป็นเอกสารส่วนหนึ่งของสัญญา

13. อัตราค่าปรับ

13.1 กรณีระบบที่ให้เช่าตามสัญญานี้เกิดการขัดข้องไม่สามารถให้บริการได้ส่วนหนึ่งของระบบ หรือทั้งหมดโดยไม่ได้เกิดจากความผิดพลาดของ กทท. ให้ผู้ให้เช่าดำเนินการแก้ไขซ่อมแซมให้แล้วเสร็จภายใน 1 ชั่วโมง หากเกินเวลาจากนั้นผู้ให้เช่าต้องชำระค่าปรับให้แก่ กทท. เป็นรายชั่วโมงในอัตราร้อยละ 0.2 (ศูนย์จุดสอง) ของราคาค่าเช่าทั้งหมดรวมภาษีมูลค่าเพิ่ม โดยเริ่มนับจากวันและเวลาที่ กทท. แจ้งไปจนถึงวันและเวลาที่ดำเนินการแก้ไขเสร็จเรียบร้อย การคำนวณค่าปรับจะนับเศษของนาทีเป็น 1 ชั่วโมง

13.2 กรณีมีการขัดข้องของระบบที่ให้เช่า นับเวลาการขัดข้องแต่ละครั้ง รวมเวลาการขัดข้องเป็นจำนวนมากกว่า 24 (ยี่สิบสี่) ชั่วโมง ในแต่ละเดือน กทท. ขอสงวนสิทธิ์ที่จะไม่จ่ายเงินค่าเช่าบริการในเดือนนั้น ๆ

13.3 หากเกิดการโจมตีของภัยคุกคาม โดยระบบฯ ไม่สามารถป้องกันได้ ผู้ให้เช่าต้องรีบดำเนินการแก้ไขสถานการณ์ดังกล่าวให้แล้วเสร็จภายใน 6 ชั่วโมง นับถัดจากที่ กทท. แจ้งเหตุ หากเกินเวลาจากนั้นผู้ให้เช่าต้องชำระค่าปรับให้แก่ กทท. เป็นรายชั่วโมงในอัตราร้อยละ 0.2 (ศูนย์จุดสอง) ของราคาค่าเช่าทั้งหมดรวมภาษีมูลค่าเพิ่ม โดยเริ่มนับจากวันและเวลาที่ กทท. แจ้งไปจนถึงวันและเวลาที่ดำเนินการแก้ไขเสร็จเรียบร้อย การคำนวณค่าปรับจะนับเศษของนาทีเป็น 1 ชั่วโมง

13.4 ในกรณีอื่น ๆ ที่ขอบเขตของงานในแต่ละหัวข้อไม่ได้ระบุถึงอัตราค่าปรับไว้ หากผู้ให้เช่าไม่ปฏิบัติตามขอบเขตของงานข้อใดข้อหนึ่งตามที่กำหนดไว้นั้น กทท. ขอสงวนสิทธิ์ในการปรับเป็นรายวัน ในอัตราร้อยละ 0.2 (ศูนย์จุดสอง) ของราคาค่าเช่าทั้งหมด โดยนับจากวันที่ได้รับแจ้งจาก กทท. จนถึงวันที่ดำเนินการแล้วเสร็จ

14. ความรับผิดของผู้ให้เช่า

ผู้ให้เช่าจะต้องรับผิดต่อผู้เช่าในกรณีที่ผู้ให้เช่า ผู้แทน ช่าง หรือลูกจ้าง ของผู้ให้เช่าจงใจหรือประมาทเลินเล่อ หรือไม่มีความรู้ความชำนาญพอ กระทำหรืองดเว้นการกระทำใด ๆ เป็นเหตุให้คอมพิวเตอร์หรืออุปกรณ์ต่าง ๆ ของผู้เช่าเสียหายหรือไม่อยู่ในสภาพที่ใช้การได้ดี โดยไม่อาจแก้ไขได้ โดยผู้ให้เช่าจะต้องจัดหาคอมพิวเตอร์หรืออุปกรณ์ที่มีคุณภาพและความสามารถในการใช้งานไม่ต่ำกว่าของเดิมชดใช้แทน หรือชดใช้ราคาคอมพิวเตอร์หรืออุปกรณ์ในกรณีที่ไม่อาจจัดหาคอมพิวเตอร์หรืออุปกรณ์ดังกล่าวชดใช้แทนได้ ให้แก่ผู้เช่าภายในเวลาที่ผู้เช่ากำหนด

หากผู้ให้เช่าดำเนินการไม่แล้วเสร็จภายในเวลาที่ผู้เช่ากำหนด ผู้ให้เช่าต้องยินยอมให้ผู้เช่าปรับเป็นรายวันในอัตราร้อยละ 0.1 (ศูนย์จุดหนึ่ง) ของราคาอุปกรณ์ดังกล่าวนี้ นับตั้งแต่เวลาที่ผู้เช่าบอกกล่าวให้ผู้ให้เช่าจัดหาคอมพิวเตอร์หรืออุปกรณ์มาชดใช้ให้แทน หรือชดใช้ราคาคอมพิวเตอร์หรืออุปกรณ์ต่าง ๆ จนถึงวันเวลาที่ดำเนินการแล้วเสร็จ หรือผู้เช่าบอกเลิกสัญญา (การคิดค่าปรับจะนับ 24 ชั่วโมงเป็น 1 วัน โดยเศษที่ไม่ครบ 24 ชั่วโมงนับเป็น 1 วัน) และหากผู้เช่าต้องใช้อุปกรณ์อื่นมาดำเนินการแทน ผู้ให้เช่าต้องยินยอมชดใช้ค่าใช้จ่ายในการดำเนินการทั้งสิ้นแทนผู้เช่าอีกด้วย

นอกจากนี้ ผู้ให้เช่าจะต้องรับผิดชอบต่ออุบัติเหตุ ความเสียหาย หรือภยันตรายใด ๆ อันเกิดจากการปฏิบัติงานของผู้ให้เช่า และต้องรับผิดต่อความเสียหายจากการกระทำหรืองดเว้นกระทำโดยผิดกฎหมายหรือโดยจงใจหรือประมาทเลินเล่อของผู้แทน ช่าง หรือลูกจ้างของผู้ให้เช่าอีกด้วย

1. ..... 2. ..... 3. ..... 4. ..... 5. .....

15. การบอกเลิกสัญญา

ในกรณีที่ กทท. พิจารณาแล้วเห็นว่า การให้เช่าระบบฯ ของผู้ให้เช่าไม่เป็นไปตามสัญญา กทท. มีสิทธิบอกเลิกสัญญาเสียเมื่อไรก็ได้ ผู้ให้เช่าจะต้องชดใช้ค่าเสียหายที่เกิดขึ้นตามสัญญาไม่ว่าทางตรงหรือทางอ้อมให้แก่ กทท. และจะพิจารณาให้เป็นผู้ทิ้งงานตามระเบียบของทางราชการด้วย

16. ข้อสงวนสิทธิ์

16.1 ในกรณีที่บุคคลภายนอกกล่าวอ้างหรือใช้สิทธิ์เรียกร้องใด ๆ ว่ามีการละเมิดลิขสิทธิ์ หรือสิทธิบัตรเกี่ยวกับระบบที่เสนอในงานเช่านี้ ผู้ให้เช่าต้องดำเนินการทั้งปวง เพื่อให้การกล่าวอ้างหรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว โดยผู้ให้เช่าต้องเป็นผู้ชำระค่าเสียหายและค่าใช้จ่ายต่าง ๆ ที่เกิดขึ้นทั้งหมด

16.2 ในกรณีที่ กทท. มีความจำเป็นต้องปรับเปลี่ยนหรือแก้ไขการติดตั้งหรือปรับตั้งค่าระบบฯ ที่ได้ติดตั้งไว้เรียบร้อยแล้ว ผู้ให้เช่าต้องดำเนินการปรับปรุงหรือแก้ไขตามที่ กทท. ร้องขอ รวมถึงการจัดหาระบบ และ/หรืออุปกรณ์อื่นใดเพิ่มเติมจากที่ได้เสนอไว้ก่อนหน้านี้ เพื่อให้ระบบสามารถทำงานได้อย่างมีประสิทธิภาพ ผู้ให้เช่าจะต้องดำเนินการจัดหาพร้อมติดตั้งเพิ่มเติมให้แก่ กทท. โดยไม่คิดค่าใช้จ่ายเพิ่มเติมจาก กทท.

16.3 ในกรณีที่ กทท. พิจารณาแล้วไม่มีความจำเป็นในการเช่าใช้งานระบบฯ ตามสัญญานี้ทั้งหมดหรือบางส่วน กทท. ขอสงวนสิทธิ์ที่จะยกเลิกสัญญาดังกล่าวนี้ โดย กทท. จะแจ้งให้คู่สัญญาทราบอย่างเป็นลายลักษณ์อักษรล่วงหน้าเป็นเวลาไม่น้อยกว่า 30 วัน

17. วงเงินงบประมาณ

วงเงินงบประมาณที่ได้รับจัดสรร 3,852,000.- บาท (สามล้านแปดแสนห้าหมื่นสองพันบาทถ้วน)

18. ความต้องการด้านความปลอดภัยสารสนเทศ

ผู้ให้เช่าต้องยินยอมปฏิบัติตาม คำสั่ง นโยบาย และแนวปฏิบัติของ กทท. โดยสามารถอ่านได้จากเว็บไซต์ กทท. (www.port.co.th) ดังต่อไปนี้

18.1 นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ ของ กทท.

18.2 แนวปฏิบัติในการใช้อาคารฝ่ายเทคโนโลยีสารสนเทศและห้อง Data Center ของ กทท.

18.3 นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ กทท.

ภาคผนวก ก.

ระบบตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์ ต้องมีคุณลักษณะเฉพาะดังต่อไปนี้

1. เป็นระบบรักษาความปลอดภัยที่สามารถติดตั้ง Agent และทำงานบนระบบปฏิบัติการ Microsoft Windows Server 2008 R2, Microsoft Windows Server 2012, 2016, 2019, 2022 รวมถึงรองรับระบบปฏิบัติการอื่น ๆ อาทิ เช่น Solaris 11, Debian Linux 9, RedHat Enterprise Linux 6, 7, Ubuntu Linux (LTS), SUSE Enterprise Linux 12
2. สามารถเชื่อมต่อกับ VMware vCenter เพื่อค้นหา (Discover) Workload หรือ Virtual Machine ที่ทำงานอยู่ได้
3. มีความสามารถตรวจสอบ Malware ด้วยเทคโนโลยี Definition, Machine Learning และ Behavior Monitor เพื่อป้องกัน Malware ที่เกิดใหม่ได้
4. สามารถป้องกัน Ransomware บนแพลตฟอร์ม Windows ได้ด้วยการเฝ้าระวังพฤติกรรม (Behavior)
5. สามารถป้องกัน Docker Container โดยวิธีการตรวจหา Malware ในไฟล์ที่ถูกเขียนผ่าน Docker บนแพลตฟอร์ม Linux ได้ หรือทำ Network Segmentation สำหรับ Docker หรือทำ Docker Sandbox ได้
6. มีความสามารถในการทำ Firewall ในลักษณะของ Host-based Firewall ได้
7. มีความสามารถในการป้องกันช่องโหว่ของระบบปฏิบัติการทางเครือข่ายได้ (Intrusion Prevention System, Host-Based Intrusion, HIPS)
8. สามารถสแกนเครื่องคอมพิวเตอร์เพื่อหา Vulnerable Software และปรับตั้งค่า Recommended Security ที่เหมาะสมให้ หรือนำเสนอ Vulnerability Assessment Tool ที่มีลิขสิทธิ์การทำงานถูกต้องเพื่อตรวจหา Vulnerable Software บนเครื่องคอมพิวเตอร์ปลายทาง โดยต้องมีการอัพเดทฐานข้อมูลให้มีความทันสมัยตลอดอายุการใช้งานได้
9. มีความสามารถในการป้องกันการโจมตีในระดับ Application Layer อาทิเช่น SQL injection และ Cross-Site Script และสามารถทำ SSL Inspection ได้ หรือสามารถเสนออุปกรณ์อื่นเพื่อเสริมความสามารถดังกล่าวที่มี Throughput ไม่ต่ำกว่า 4 Gbps ได้
10. สามารถตรวจจับและป้องกันช่องโหว่ประเภท Zero-day Vulnerabilities ได้ โดยรวมถึง Exploits ประเภทต่าง ๆ ด้วย
11. ระบบจะต้องทำการเฝ้าระวังการเปลี่ยนแปลง (Integrity Monitoring) Files และ Registry ได้เป็นอย่างน้อย
12. สามารถทำ Application Control เพื่อบล็อคการทำงานแอพพลิเคชั่นแปลกปลอมบน Windows และ Linux OS ได้
13. สามารถวิเคราะห์ Log File ของระบบปฏิบัติการณ์หรือแอพพลิเคชั่นต่าง ๆ (Log Inspect หรือ Log Monitor หรือ Logon Tracker) และแจ้งเตือนถึงเหตุการณ์น่าสงสัย (Suspicious Activity) หรือเหตุการณ์เกี่ยวกับความปลอดภัยของระบบที่ใช้งานได้
14. เจ้าของผลิตภัณฑ์ต้องได้รับการจัดอันดับอยู่ในกลุ่ม Leaders หรือ Strong Performers ของ Forrester Wave Endpoint Security ปี 2023 หรือใหม่กว่า
15. สามารถตรวจสอบและวิเคราะห์ภัยคุกคามแบบ Extended Detection and Response (XDR) ได้ ดังนี้
    15.1 สามารถบันทึกหลักฐานต่าง ๆ ของเครื่องคอมพิวเตอร์ (Telemetry หรือ Forensic Analysis) เพื่อตรวจสอบเหตุการณ์การทำงานของ Malware ได้ย้อนหลังไม่น้อยกว่า 30 วัน และสามารถดูการแจ้งเตือนเหตุการณ์ย้อนหลังได้ไม่น้อยกว่า 180 วัน

1. ..... 2. ..... 3. ..... 4. ..... 5. .....

15.2 สามารถบันทึกและตรวจสอบสิ่งที่เกิดขึ้น เช่น File หรือ Process หรือ Network Communication หรือ Network Events ได้

15.3 สามารถทำงาน Response เช่น Isolate Endpoint ได้

15.4 สามารถทำงานค้นหาร่องรอยการโจมตี (Sweeping / Hunting) จากข้อมูลที่บันทึก โดยมี Threat Intelligence จากเจ้าของผลิตภัณฑ์เองและสามารถเพิ่มแหล่งข้อมูลจาก STIX File, TAXII Feeds ได้

15.5 สามารถทำ Security Playbook เพื่อจัดการความเสี่ยงที่เกิดขึ้นได้โดยอัตโนมัติ

15.6 สามารถแสดงผลความเสี่ยงขององค์กรหรือช่องทางการโจมตี (Attack Surface) โดยพิจารณาถึงปัจจัยภายนอกเช่น Internet Facing IP Address หรือ Internet Facing Assets และช่องโหว่ CVE ได้ และปัจจัยภายในเช่นความเสี่ยงจาก User Accounts (Identities) และ Devices Vulnerabilities ได้

15.7 เจ้าของผลิตภัณฑ์ต้องได้รับการจัดอันดับอยู่ในกลุ่ม Leaders หรือ Strong Performers ของ Forrester New Wave XDR Providers ปี 2023 หรือใหม่กว่า

1. ..... 2. ..... 3. ..... 4. ..... 5. .....

ภาคผนวก ข.

<u>รายละเอียดระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายของ กทท.</u>

- Windows server 2003 / 2003 R2
- Microsoft Windows Server 2008 / 2008 R2
- Microsoft Windows Server 2012 / 2012 R2
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Oracle Solaris 11
- Oracle Linux 8
- Ubuntu Linux 18.04 / 20.04 / 22.04
- Red Hat Enterprise Linux 6 / 7 / 8
- SUSE Linux Enterprise 11
- CentOS 4 / 5

ประมาณราคากลาง

เช่าใช้ระบบตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์ของระบบเครื่องคอมพิวเตอร์แม่ข่าย เป็นระยะเวลา 12 เดือน

รายการ	ค่าจ้างบริการรายเดือน (บาท)	ค่าจ้างบริการรวม 12 เดือน (บาท)
เช่าใช้ระบบตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์ของระบบเครื่องคอมพิวเตอร์แม่ข่าย	297,500.00	3,570,000.00
	ภาษีมูลค่าเพิ่ม 7%	249,900.00
	รวมเป็นเงินทั้งสิ้น	3,819,900.00

1. ..... 2. ..... 3. ..... 4. ..... 5. .....

กทท. การท่าเรือแห่งประเทศไทย

ใบเสนอราคา

เช่าใช้ระบบตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์ของระบบเครื่องคอมพิวเตอร์แม่ข่าย เป็นระยะเวลา 12 เดือน

รายการ	ค่าจ้างบริการรายเดือน (บาท)	ค่าจ้างบริการรวม 12 เดือน (บาท)
เช่าใช้ระบบตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์ของระบบเครื่องคอมพิวเตอร์แม่ข่าย		
ภาษีมูลค่าเพิ่ม 7%		
รวมเป็นเงินทั้งสิ้น		

1. ..... 2. ..... 3. ..... 4. ..... 5. .....