ตลาดหลักทรัพย์แห่งประเทศไทย

ประกาศเชิญชวนประกวดราคา โครงการจัดจ้าง Managed Security Services

ตลาดหลักทรัพย์แห่งประเทศไทย (“ตลาดหลักทรัพย์”) มีความประสงค์จะสรรหา คัดเลือกผู้รับจ้างงานโครงการจัดจ้าง Managed Security Services โดยมีรายละเอียดข้อมูลโครงการฯ ขอบเขตงานตามสัญญา คุณสมบัติของผู้ยื่นข้อเสนองาน กำหนดการและข้อมูลอื่นที่เกี่ยวข้องตามที่แสดงไว้ในข้อกำหนดและขอบเขตของงาน (Term of Reference) (ซึ่งต่อไปในเอกสารนี้จะเรียกว่า “ข้อกำหนดการเสนองาน”)

ข้อกำหนด

1. ความต้องการด้านเทคนิค
   a) ต้องมีศูนย์เฝ้าระวัง (Security Operation Center – SOC) ในพื้นที่ Asia Pacific Japan (APJ) เป็นอย่างน้อย
   b) ผู้ให้บริการต้องมี SOC อย่างน้อย 1 แห่ง โดย SOC แต่ละแห่งจะต้องมีศูนย์คอมพิวเตอร์เพื่อรองรับการให้บริการอย่างน้อย 2 แห่ง
   c) SOC หรือศูนย์คอมพิวเตอร์ที่ให้บริการ จะต้องได้รับการรับรองมาตรฐานสากล ISO27001 เป็นอย่างน้อย หากมีมาตรฐานอื่นเพิ่มเติม (โปรดระบุ) เช่น SSAE 16 Reporting Standard สำหรับ SOC, Certified PCI DSS v2.0 Service Provider
   d) มีทีมงาน Security Professional ที่ปฏิบัติงานใน SOC และได้รับประกาศนียบัตรในระดับ GIAC Certified Analysts หรือระดับ Cybersecurity Analyst/Forensic จำนวน 2 ท่านขึ้นไป หากมีใบประกาศนียบัตรอื่นเพิ่มเติม (โปรดระบุ)
   e) มีฐานข้อมูลภัยคุกคามเทคโนโลยีสารสนเทศและปรับปรุงให้ทันสมัยอยู่เสมอ (โปรดระบุแหล่งที่มาของฐานข้อมูล)
   f) มีระบบ Ticket Management เพื่อบริหารจัดการและติดตามเหตุการณ์ภัยคุกคามด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศที่เกิดขึ้นได้
   g) จัดเตรียมอุปกรณ์และเครือข่ายในการเชื่อมต่อระหว่างตลาดหลักทรัพย์และผู้ให้บริการ SecureWorks
2. การดำเนินงาน และสิ่งที่ต้องส่งมอบ
   a) ให้บริการเฝ้าระวังภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ แบบ 24x7x365 (ตลอดเวลา) โดยมี Availability SLA ≥ 99.95%
   b) ต้องสามารถวิเคราะห์ Log จากอุปกรณ์ต่างๆ ทั้งระดับ Application และ Systems ซึ่งติดตั้งใช้งานที่ศูนย์คอมพิวเตอร์ของตลาดหลักทรัพย์ทั้ง 2 แห่ง โดยมีรายการเบื้องต้น อย่างน้อยดังนี้
      - Firewall with IPS/IDS features (Active-Standby) จำนวน 6 ตัว
      - Load-balance (Active-Standby) จำนวน 4 ตัว
      - Proxy จำนวน 4 อุปกรณ์
      - VPN จำนวน 2 ตัว
      - Active Directory/LDAP

      ผู้เสนอราคาสามารถนำเสนอราคาการวิเคราะห์ Log จากอุปกรณ์อื่นเพิ่มเติม (Optional) เช่น Antivirus/ Anti-malware เป็นต้น อีกทั้งตลาดหลักทรัพย์ขอสงวนสิทธิ์ในการเปลี่ยนแปลงรายการ Log จากที่ระบุในข้อนี้เป็นอุปกรณ์อื่นในประเภทเดียวกันในจำนวนที่เท่ากัน โดยไม่มีค่าใช้จ่ายเพิ่มเติม
   c) ให้บริการวิเคราะห์ข้อมูล Traffic ที่มีความเสี่ยงเป็นภัยคุกคามด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศได้

d) ให้บริการจัดเก็บข้อมูล Incident Log ซึ่งสามารถพร้อมใช้งานได้ตลอดเวลาตามการร้องขอของตลาดหลักทรัพย์โดยรองรับความต้องการดังต่อไปนี้
   - สามารถเรียกแสดงผล Incident Log ย้อนหลังไม่น้อยกว่า 3 เดือน
   - มีการสำรองข้อมูล Incident Log ไว้เป็นระยะเวลาไม่น้อยกว่า 12 เดือน

e) ใช้วิธีวิเคราะห์ข้อมูลภัยคุกคามด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ โดยดำเนินการที่ตลาดหลักทรัพย์ทั้งหมด หรือดำเนินที่ SOC ทั้งหมด หรือมีวิธีการดำเนินการในรูปแบบอื่น (โปรดระบุ)

f) จัดเตรียมช่องทางการจัดส่ง Log จากศูนย์คอมพิวเตอร์ทั้ง 2 แห่งของตลาดหลักทรัพย์กับ SOC ของผู้ให้บริการ โดยต้องมีการบริหารจัดการช่องทางการจัดส่ง Log ไปยัง SOC ให้มีประสิทธิภาพและปลอดภัย ดังนี้

g) รองรับการบีบอัดและการเข้ารหัสข้อมูล

h) สามารถจำกัด Bandwidth ในการส่งข้อมูลได้ (Optional)

i) วิธีการจัดการอื่นๆ เพื่อเพิ่มประสิทธิภาพและความปลอดภัย (โปรดระบุ)

j) ให้คำปรึกษาหรือแก้ปัญหาเบื้องต้นในแต่ละ Incident กับเจ้าหน้าที่ตลาดหลักทรัพย์ โดยทีมงานผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Security Analysts) ได้ตลอดเวลา (24x7x365) โดยไม่กำหนดจำนวนครั้ง และไม่จำกัดเวลา ผ่านช่องทางต่างๆ เช่น โทรศัพท์, E-mail, Web Chat, Instant Messaging, On-site support/forensic เป็นต้น (โปรดระบุ)

k) หากพบเหตุการณ์ที่กระทบความมั่นคงปลอดภัยในระดับ Critical Event จะต้องแจ้งให้แก่เจ้าหน้าที่ของตลาดหลักทรัพย์ทราบผ่านช่องทางโทรศัพท์ และ E-mail เป็นอย่างน้อย พร้อมคำแนะนำและข้อมูลประกอบในการบริหารจัดการปัญหา ภายใน 15 นาที (SLA) นับจากเวลาที่ตรวจพบเหตุการณ์ดังกล่าวในอุปกรณ์ของตลาดหลักทรัพย์

l) มีทีมงานที่ทำหน้าที่วิเคราะห์ความเสี่ยงจากฐานข้อมูลภัยคุกคามเทคโนโลยีสารสนเทศ และดำเนินการให้ระบบเฝ้าระวังภัยคุกคามสามารถตรวจจับภัยคุกคามที่เกิดจากความเสี่ยงดังกล่าว

3. การส่งมอบและการติดตั้ง
   a) ตั้งค่าระบบเพื่อนำข้อมูล log จากอุปกรณ์ต่างๆเข้าสู่ระบบการเฝ้าระวังติดตามของ Securework
   b) จัดทำรายงานสรุปเหตุการณ์ที่เกิดขึ้นพร้อมข้อเสนอแนะและข้อมูลประกอบอย่างเหมาะสม และจัดส่งอย่างสม่ำเสมออย่างน้อย 1 ครั้งต่อเดือน (โปรดระบุรูปแบบในการรายงาน) (โปรดระบุความถี่ในการจัดส่งรายงาน เช่น ต่อวัน, ต่อสัปดาห์, ต่อเดือน เป็นต้น)
   c) สำหรับการติดตั้ง Software หรืออุปกรณ์ที่ตลาดหลักทรัพย์ในการให้บริการ โปรดระบุรายละเอียดพร้อมข้อมูลแผนผัง (Diagram), การเชื่อมต่อ, การใช้งาน Port และขั้นตอนดำเนินการ
   c) กำหนดการส่งมอบระบบ ผู้เสนองานจะต้องดำเนินการภายในวันที่ 21 ธันวาคม 2561

4. การรับประกันและบำรุงรักษา

   การดูแลและบริหารจัดการอุปกรณ์หรือ Software ที่ให้บริการตลาดหลักทรัพย์จะต้องสามารถให้บริการได้ตลอด 24 ชั่วโมง โดยหากพบปัญหา ทางผู้เสนองานจะต้องเข้ามาดำเนินการแก้ไขโดย

5. ระยะเวลา

ระยะเวลาให้บริการตั้งแต่ประมาณวันที่ 1 มกราคม 2562 ถึงวันที่ 31 ธันวาคม 2563

ทั้งนี้ ข้อกำหนดมีรายละเอียดอยู่หลายข้อ โปรดอ่านรายละเอียดในเอกสารข้อกำหนดและขอบเขตของงาน (Term of Reference)

กำหนดการ

ลำดับ	รายละเอียด	กำหนดการ
1.	ประกาศเชิญชวน	29 พฤศจิกายน 2561
2.	สอบถามข้อมูลเพิ่มเติมเป็นลายลักษณ์อักษรทางอีเมล์ ITProcurementUnit@set.or.th	3 ธันวาคม 2561
3.	กำหนดตอบคำถามเป็นลายลักษณ์อักษร	5 ธันวาคม 2561
4.	ยื่นซองประกวดราคา	18 ธันวาคม 2561 ก่อนเวลา 17.00 น.
5.	ประกาศรายชื่อผู้ชนะการประกวดราคา	26 ธันวาคม 2561

หมายเหตุ ตลาดหลักทรัพย์ขอสงวนสิทธิในการเปลี่ยนแปลงกำหนดการดังกล่าวข้างต้นได้ตามความเหมาะสม

ประกาศ ณ วันที่ 29 พฤศจิกายน 2561

ติดต่อสอบถามข้อมูลเพิ่มเติม

Email: itprocurementunit@set.or.th

ฝ่ายจัดซื้อ ส่วนจัดซื้อเทคโนโลยีสารสนเทศ

ชั้นที่ 17 อาคารตลาดหลักทรัพย์แห่งประเทศไทย ถนนรัชดาภิเษก ดินแดง กรุงเทพฯ

Visit us at http://www.set.or.th