ตลาดหลักทรัพย์แห่งประเทศไทย

ประกาศเชิญชวนประกวดราคา โครงการ Managed Security Services

ตลาดหลักทรัพย์แห่งประเทศไทย มีความประสงค์จะสรรหา คัดเลือกผู้รับจ้างงาน โครงการ Managed Security Services รวมทั้งให้บริการที่เกี่ยวข้อง ให้แก่ตลาดหลักทรัพย์ รวมตลอดถึงบริษัทย่อยของตลาดหลักทรัพย์ให้แล้วเสร็จสมบูรณ์ ตามรายละเอียดที่กำหนดในข้อกำหนดและขอบเขตของงาน ภายในระยะเวลาที่กำหนดและราคาที่ตกลงกัน เพื่อให้ได้ผลงานที่ดี มีคุณภาพ ตามวัตถุประสงค์ของการใช้งานและเงื่อนไขของสัญญา

ข้อกำหนด

1. ให้บริการเฝ้าระวังภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ แบบ 24x7x365 (ตลอดเวลา) โดยมี Availability SLA ≥ 99.95% และระยะเวลาให้บริการตั้งแต่ประมาณวันที่ 1 พฤศจิกายน 2560 ถึงวันที่ 31 ธันวาคม 2561 ทั้งนี้ตลาดหลักทรัพย์ขอสงวนสิทธิ์ในการเปลี่ยนแปลงระยะเวลาการใช้บริการตามความเหมาะสม

2. ต้องมีศูนย์เฝ้าระวัง (Security Operation Center – SOC) ในพื้นที่ Asia Pacific Japan (APJ) เป็นอย่างน้อย

3. SOC หรือศูนย์คอมพิวเตอร์ที่ให้บริการ จะต้องได้รับการรับรองมาตรฐานสากล ISO27001 เป็นอย่างน้อย หากมีมาตรฐานอื่นเพิ่มเติม (โปรดระบุ) เช่น SSAE 16 Reporting Standard สำหรับ SOC, Certified PCI DSS v2.0 Service Provider

4. ผู้ให้บริการต้องมี SOC อย่างน้อย 1 แห่ง โดย SOC แต่ละแห่งจะต้องมีศูนย์คอมพิวเตอร์เพื่อรองรับการให้บริการอย่างน้อย 2 แห่ง

5. มีทีมงาน Security Professional ที่ปฏิบัติงานใน SOC และได้รับประกาศนียบัตรในระดับ GIAC Certified Analysts หรือระดับ Cybersecurity Analyst/Forensic จำนวน 2 ท่านขึ้นไป หากมีใบประกาศนียบัตรอื่นเพิ่มเติม (โปรดระบุ) ต้องสามารถวิเคราะห์ Log จากอุปกรณ์ต่างๆ ซึ่งติดตั้งใช้งานที่ศูนย์คอมพิวเตอร์ของตลาดหลักทรัพย์ทั้ง 2 แห่ง โดยมีรายการเบื้องต้น ดังนี้

   a. Firewall with IPS/IDS features (Active-Standby) จำนวน 3 คู่
   b. Load-balance (Active-Standby) จำนวน 2 คู่
   c. Proxy จำนวน 4 อุปกรณ์
   d. VPN จำนวน 2 อุปกรณ์

   ผู้เสนอราคาสามารถนำเสนอราคาการวิเคราะห์ Log จากอุปกรณ์อื่นเพิ่มเติม (Optional) เช่น Antivirus/ Anti-malware, Active Directory/LDAP

6. ตลาดหลักทรัพย์ขอสงวนสิทธิ์ในการเปลี่ยนแปลงรายการ Log จากที่ระบุในข้อ 2.5 เป็นอุปกรณ์อื่นในลักษณะเดียวกัน ในจำนวนที่เท่ากัน โดยไม่มีค่าใช้จ่ายเพิ่มเติม เช่น เปลี่ยน Log ของอุปกรณ์ Firewall ยี่ห้อ A เป็น B, เปลี่ยน Log ของ Server ระบบปฏิบัติการ X เป็น Y

7. ให้บริการวิเคราะห์ข้อมูล Log ที่มีความเสี่ยงเป็นภัยคุกคามด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศได้ โดยทีมงาน Security Professional

8. ให้บริการจัดเก็บข้อมูล Incident Log เป็นระยะเวลาไม่น้อยกว่า_12 เดือน ซึ่งสามารถพร้อมใช้งานได้ตลอดเวลาตามการร้องขอของตลาดหลักทรัพย์โดยรองรับความต้องการดังต่อไปนี้

   a. สามารถเรียกผล Incident Log ย้อนหลังไม่น้อยกว่า 3 เดือน
   b. มีการสำรองข้อมูล Incident Log เพิ่มเติมให้เป็นไปตามที่กำหนดไว้

9. ใช้วิธีวิเคราะห์ข้อมูลภัยคุกคามด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ โดยดำเนินการที่ตลาดหลักทรัพย์ทั้งหมด หรือดำเนินที่ SOC ทั้งหมด หรือมีวิธีการดำเนินการในรูปแบบอื่น (โปรดระบุ)

10. จัดหาและติดตั้งอุปกรณ์พร้อม License ที่เกี่ยวข้องทั้งหมด รวมทั้งช่องทางการเชื่อมต่อระหว่างศูนย์คอมพิวเตอร์ทั้ง 2 แห่งของตลาดหลักทรัพย์กับ SOC ของผู้ให้บริการ โดยต้องมีการบริหารจัดการช่องดังกล่าวให้มีประสิทธิภาพและปลอดภัย ดังนี้

   a. รองรับการบีบอัดและการเข้ารหัสข้อมูล
   b. สามารถจำกัด Bandwidth ในการส่งข้อมูลได้ (Optional)
   c. วิธีการจัดการอื่นๆ เพื่อเพิ่มประสิทธิภาพและความปลอดภัย (โปรดระบุ)

11. 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)

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

13. มีฐานข้อมูลภัยคุกคามเทคโนโลยีสารสนเทศและปรับปรุงให้ทันสมัยอยู่เสมอ (โปรดระบุแหล่งที่มาของฐานข้อมูล)

14 มีทีมงานที่ทำหน้าที่วิเคราะห์ความเสี่ยงจากฐานข้อมูลภัยคุกคามเทคโนโลยีสารสนเทศ และดำเนินการให้ระบบเฝ้าระวังภัยคุกคามสามารถตรวจจับภัยคุกคามที่เกิดจากความเสี่ยงดังกล่าว

15. มีระบบ Ticket Management เพื่อบริหารจัดการและติดตามเหตุการณ์ภัยคุกคามด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศที่เกิดขึ้นได้

16. จัดทำรายงานสรุปเหตุการณ์ที่เกิดขึ้นพร้อมข้อเสนอแนะและข้อมูลประกอบอย่างเหมาะสม และจัดส่งอย่างสม่ำเสมออย่างน้อย 1 ครั้งต่อเดือน (โปรดระบุรูปแบบในการรายงาน) (โปรดระบุความถี่ในการจัดส่งรายงาน เช่น ต่อวัน, ต่อสัปดาห์, ต่อเดือน เป็นต้น)

17. ในการให้บริการ หากมีความจำเป็นต้องติดตั้ง Software หรืออุปกรณ์ที่ตลาดหลักทรัพย์ โปรดระบุรายละเอียด พร้อมข้อมูลแผนผัง (Diagram), การเชื่อมต่อ, การใช้งาน Port และขั้นตอนดำเนินการ

18. จัดให้ให้ผู้แทนตลาดหลักทรัพย์อย่างน้อย 1 ท่าน เข้าตรวจประเมินการให้บริการ ณ ศูนย์การดำเนินงานของ SOC ได้ตามที่ตลาดหลักทรัพย์ร้องขอ จำนวน 1 ครั้ง โดยผู้ให้บริการมีหน้าที่รับผิดชอบค่าใช้จ่ายที่เกิดขึ้นจากการเข้าตรวจประเมิน ได้แก่ ค่าเดินทาง ค่าที่พัก (ถ้ามี)

ทั้งนี้ ข้อกำหนดมีรายละเอียดอยู่หลายข้อ โปรดอ่านรายละเอียดในเอกสารข้อกำหนดและขอบเขตของงาน (Term of Reference)

กำหนดการ

รับข้อกำหนดการเสนองาน	1 กันยายน 2560
กำหนดรับคำถาม	4 สิงหาคม 2560 – 8 กันยายน 2560
กำหนดตอบคำถาม	11 กันยายน 2560 – 12 กันยายน 2560
ยื่นซองข้อเสนองาน	15 กันยายน 2560 ภายในไม่เกินเวลา 17:00
แจ้งผลผู้ชนะการคัดเลือก	ภายหลังวันที่ 22 กันยายน 2560

หมายเหตุ ตลาดหลักทรัพย์ขอสวงนสิทธิในการเปลี่ยนแปลงกำหนดการดังกล่าวข้างต้นได้ตามความเหมาะสม

ประกาศ ณ วันที่ 1 กันยายน 2560

ติดต่อสอบถามข้อมูลเพิ่มเติม

Email: itprocurementunit@set.or.th

ฝ่ายจัดซื้อ ส่วนจัดซื้อเทคโนโลยีสารสนเทศ

ชั้นที่ 17 อาคารตลาดหลักทรัพย์แห่งประเทศไทย ถนนรัชดาภิเษก ดินแดง กรุงเทพฯ Visit us at http://www.set.or.th