ตลาดหลักทรัพย์แห่งประเทศไทย

ประกาศเชิญชวนประกวดราคา

โครงการจัดหาบริการ Managed Security Services

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

ข้อกำหนด

1. งานตามสัญญา

1.1 ความต้องการด้านเทคนิค

a) ต้องมีศูนย์เฝ้าระวัง (Security Operation Center - SOC) ในพื้นที่ Asia Pacific Japan (APJ) เป็นอย่างน้อย โดย SOC แต่ละแห่งจะต้องมีศูนย์คอมพิวเตอร์เพื่อรองรับการให้บริการอย่างน้อย 2 แห่ง

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

c) มีทีมงาน Security Professional ที่ปฏิบัติงานใน SOC และได้รับประกาศนียบัตรในระดับ GIAC Certified Analysts หรือระดับ Cyber security Analyst/Forensic จำนวน 10 ท่านขึ้นไป หากมีใบประกาศนียบัตรอื่นเพิ่มเติม (โปรดระบุ)

d) มีฐานข้อมูลภัยคุกคามเทคโนโลยีสารสนเทศและปรับปรุงให้ทันสมัยอยู่เสมอ (โปรดระบุแหล่งที่มาของฐานข้อมูล)

e) มีระบบ Ticket Management เพื่อบริหารจัดการและติดตามเหตุการณ์ภัยคุกคามด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศที่เกิดขึ้นได้

f) มีการจัดเตรียมอุปกรณ์และเครือข่ายในการเชื่อมต่อ (Internet Link) ระหว่างตลาดหลักทรัพย์และผู้ให้บริการ SecureWorks

g) มีระบบการจัดทำรายงานที่เกี่ยวกับภัยคุกคามที่เกี่ยวข้องย้อนหลังได้ 90 วัน

h) Global Threat Intelligence Visibility and Insight

1.2 การดำเนินงาน และสิ่งที่ต้องส่งมอบ

a) ให้บริการเฝ้าระวังภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศแบบ 24x7x365 (ตลอดเวลา)โดยมี Availability SLA ไม่ต่ำกว่า 99.95%

b) ต้องสามารถวิเคราะห์ Log จากอุปกรณ์ต่างๆ ทั้งระดับ Applications และ Systems ซึ่งติดตั้งใช้งานที่ศูนย์คอมพิวเตอร์ของตลาดหลักทรัพย์ โดยรองรับอุปกรณ์เบื้องต้นดังนี้

- อุปกรณ์ Network/Firewall/IPS/IDS จำนวน 10 คู่
- อุปกรณ์ Server จำนวน 40 เครื่อง
- สิทธิในการตรวจจับภัยคุกคามทางเทคโนโลยีสารสนเทศ (Endpoint Threat Detection) ในระบบ 40 Licenses

อีกทั้งตลาดหลักทรัพย์ขอสงวนสิทธิ์ในการเปลี่ยนแปลงรายการ Log จากที่ระบุในข้อนี้เป็นอุปกรณ์อื่นในประเภทเดียวกันในจำนวนที่เท่ากันโดยไม่มีค่าใช้จ่ายเพิ่มเติม

c) ให้บริการวิเคราะห์ข้อมูล Traffic ที่มีความเสี่ยงเป็นภัยคุกคามด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศได้
d) ให้บริการจัดเก็บข้อมูล Incident Log ซึ่งสามารถพร้อมใช้งานได้ตลอดเวลาตามการร้องขอของตลาดหลักทรัพย์ โดยรองรับความต้องการดังต่อไปนี้
    - สามารถเรียกแสดงผล Incident Log ย้อนหลังไม่น้อยกว่า 3 เดือน
    - มีการสำรองข้อมูล Incident Log ไว้เป็นระยะเวลาไม่น้อยกว่า 12 เดือน
    - ใช้วิธีวิเคราะห์ข้อมูลภัยคุกคามด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศโดยดำเนินการที่ตลาดหลักทรัพย์ทั้งหมดหรือดำเนินที่ SOC ทั้งหมด หรือมีวิธีการดำเนินการในรูปแบบอื่น (โปรดระบุ)
e) จัดเตรียมช่องทางการจัดส่ง Log จากศูนย์คอมพิวเตอร์ของตลาดหลักทรัพย์กับ SOC ของผู้ให้บริการ โดยต้องมีการบริหารจัดการช่องทางการจัดส่ง Log ไปยัง SOC ให้มีประสิทธิภาพและปลอดภัย ดังนี้
    - รองรับการบีบอัดและการเข้ารหัสข้อมูล
    - วิธีการจัดการอื่นๆ เพื่อเพิ่มประสิทธิภาพและความปลอดภัย (โปรดระบุ)
f) ให้คำปรึกษาหรือแก้ปัญหาเบื้องต้นในแต่ละ Incident กับเจ้าหน้าที่ตลาดหลักทรัพย์ โดยทีมงานผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Security Analysts) ได้ตลอดเวลา (24x7x365) โดยไม่กำหนดจำนวนครั้ง และไม่จำกัดเวลา ผ่านช่องทางต่างๆ เช่น โทรศัพท์, E-mail, Web Chat, Instant Messaging เป็นต้น (โปรดระบุ)
g) หากพบเหตุการณ์ที่กระทบความมั่นคงปลอดภัยในระดับ Critical Event จะต้องแจ้งให้แก่เจ้าหน้าที่ของตลาดหลักทรัพย์ทราบผ่านช่องทางโทรศัพท์ และ E-mail เป็นอย่างน้อย พร้อมคำแนะนำและข้อมูลประกอบในการบริหารจัดการปัญหาภายใน 15 นาที (SLA) นับจากเวลาที่ตรวจพบเหตุการณ์ดังกล่าวในอุปกรณ์ของตลาดหลักทรัพย์
h) มีทีมงานที่ทำหน้าที่วิเคราะห์ความเสี่ยงจากฐานข้อมูลภัยคุกคามเทคโนโลยีสารสนเทศ และดำเนินการให้ระบบเฝ้าระวังภัยคุกคามสามารถตรวจจับภัยคุกคามที่เกิดจากความเสี่ยงดังกล่าว
i) มีโปรแกรมหรือ Web Portal ที่ใช้สำหรับการสื่อสารและเชื่อมต่อไปยัง SOC ของผู้ให้บริการเพื่อให้ทางตลาดหลักทรัพย์สามารถเฝ้าติดตามและรับทราบถึงสถานะการณ์ทางด้านความปลอดภัยทางไซเบอร์ของตลาดหลักทรัพย์
j) ต้องจัดให้มีจำนวนชั่วโมงการบริการให้ความช่วยเหลือในกรณีที่มีเหตุการณ์ด้านความปลอดภัยร้ายแรงที่ต้องการการตอบสนองหรือตรวจสอบต่อเหตุการณ์ (Incident Response Services) ไม่น้อยกว่า 20 ชั่วโมง และหากกรณีที่ไม่ได้มีการนำชั่วโมงการบริการให้ความช่วยเหลือดังกล่าวมาใช้งาน สามารถนำจำนวนชั่วโมงที่เหลืออยู่นั้นมาเปลี่ยนการให้บริการแบบ Incident Response Proactive Services ได้เช่น การจัดทำนโยบายด้านความปลอดภัยต่าง ๆ เช่น Table Top Exercise, Security Process Guide or Playbook ตามความเหมาะสมของจำนวนชั่วโมงการให้บริการที่มีอยู่

ทั้งนี้ผู้เสนองานจะต้องปฏิบัติงานหรือส่งมอบงานให้เป็นตามมาตรฐานของกฎหมายหรือข้อกำหนดอื่นใดที่เกี่ยวข้อง

1.3 การส่งมอบและการติดตั้ง

a) สิทธิในการใช้บริการตามอุปกรณ์ที่กำหนดในขอบเขต

1.4 การรับประกันและบำรุงรักษา

การดูแลและบริหารจัดการอุปกรณ์หรือ Software ที่ให้บริการตลาดหลักทรัพย์จะต้องสามารถให้บริการได้ตลอด 24 ชั่วโมง โดยหากพบปัญหาทางผู้เสนองานจะต้องเข้ามาดำเนินการแก้ไข

2. ระยะเวลา

ระยะเวลาของสัญญาให้บริการ 3 ปี 6 เดือน โดยเริ่มตั้งแต่วันที่ 1 มกราคม 2565 ถึงวันที่ 30 มิถุนายน 2568

กำหนดการ

ลำดับ	รายละเอียด	กำหนดการ
1	ประกาศเชิญชวน	11 พฤศจิกายน 2564
2	สอบถามข้อมูลเพิ่มเติมเป็นลายลักษณ์อักษร ITProcurementUnit@set.or.th	16 พฤศจิกายน 2564
7	กำหนดตอบคำถามเป็นลายลักษณ์อักษร ITProcurementUnit@set.or.th	18 พฤศจิกายน 2564
8	ยื่นข้อเสนองาน	24 พฤศจิกายน 2564
10	ประกาศรายชื่อผู้ชนะการประกวดราคา	20 ธันวาคม 2564

หมายเหตุ ตลาดหลักทรัพย์ขอสงวนสิทธิในการเปลี่ยนแปลงกำหนดการดังกล่าวข้างต้นได้ตามความเหมาะสม

ติดต่อสอบถามข้อมูลเพิ่มเติม

Email: itprocurementunit@set.or.th

ฝ่ายบริหารเทคโนโลยีสารสนเทศ ส่วนจัดหาเทคโนโลยีสารสนเทศ

ชั้นที่ 10 อาคารตลาดหลักทรัพย์แห่งประเทศไทย ถนนรัชดาภิเษก ดินแดง กรุงเทพฯ Visit us at http://www.set.or.th