ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)
ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

๑. **ชื่อโครงการ :** การเช่าใช้อุปกรณ์ระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูง สำนักงาน กสทช. จำนวน ๑ ระบบ

๒. **หน่วยงานเจ้าของโครงการ** สำนักเทคโนโลยีสารสนเทศ

๓. **วงเงินงบประมาณที่ได้รับจัดสรร :** ๒๔,๔๖๒,๐๐๐.-บาท (ยี่สิบสี่ล้านสี่แสนหกหมื่นสองพันบาทถ้วน)

๔. **วันที่กำหนดราคากลาง (ราคาอ้างอิง) :** ๑๕ เมษายน ๒๕๖๓
เป็นเงิน ๒๔,๔๖๐,๙๑๓.๓๓ บาท **ราคา/หน่วย** ตามเอกสารแนบ

๕. **แหล่งที่มาของราคากลาง (ราคาอ้างอิง) :**

๕.๑ อ้างอิงใบเสนอราคาจากบริษัท เอ็น-เจนเนอเรชั่น เทคโนโลยี จำกัด เลขที่ N๑๙๐๑๐#๘ ลงวันที่ ๑ เมษายน ๒๕๖๓

๕.๒ อ้างอิงใบเสนอราคาจากบริษัท จี แอ็ดวานซ์ เทคโนโลยี จำกัด เลขที่ GAT-CAT๐๘๐-๒๕๖๓ ลงวันที่ ๓๑ มีนาคม ๒๕๖๓

๕.๓ อ้างอิงใบเสนอราคาจากบริษัท อีการ์เดียน (ประเทศไทย) จำกัด เลขที่ WI/๐๘/๒๐๒๐-๐๐๓๑B ลงวันที่ ๓๐ มีนาคม ๒๕๖๓

๖. **รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) :**

ลงชื่อ ..... ประธานกรรมการ
(นายเนติพงษ์ ตลับนาค)

ลงชื่อ ..... กรรมการ
(นายสุริยะ ธวัชวัฒนานันท์)

ลงชื่อ ..... กรรมการและเลขานุการ
(นายชัชชัย คำภักดี)

29/05/2563

ขอบเขตของงาน (Term of Reference)
เช่าใช้ระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูง
สำนักงาน กสทช. จำนวน ๑ ระบบ

๑. หลักการและเหตุผล

ด้วยสำนักเทคโนโลยีสารสนเทศสำนักงานคณะกรรมการกิจการกระจายเสียงกิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) โดยสำนักเทคโนโลยีสารสนเทศ (นบ.) มีภารกิจหลักในการสนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศให้กับหน่วยงานภายใน ทั้งส่วนกลางและส่วนภูมิภาค โดยอุปกรณ์ระบบตรวจจับและป้องกันการบุกรุกเครือข่ายใช้งานมาเป็นระยะเวลา ๕ ปีแล้ว และบริษัทผู้ผลิตได้ยกเลิกการสนับสนุน ทางสำนักงาน กสทช. จึงต้องทำการเปลี่ยนอุปกรณ์เพื่อสนับสนุนความปลอดภัยทางด้าน ระบบเครือข่าย และ ระบบคอมพิวเตอร์เสมือน ให้ทำงานมีประสิทธิภาพสูงสุด ประกอบกับจำนวนพนักงาน ลูกจ้างที่เพิ่มขึ้นทำให้ปริมาณ Current Connection Session เพิ่มขึ้นจนใกล้เต็มความสามารถสูงสุดของระบบตรวจจับและป้องกันการบุกรุกเครือข่ายที่สำนักงาน กสทช. ใช้งานอยู่ปัจจุบันนั้นรองรับได้

โดยจากเดิมอุปกรณ์ระบบตรวจจับและป้องกันการบุกรุกเครือข่ายที่สำนักงาน กสทช. ได้ซื้อมาใช้นั้น เมื่อใช้งานจนครบระยะเวลาการรับประกันแล้วต้องดำเนินการบำรุงรักษาต่อในแต่ละปีซึ่งต้องใช้ระยะเวลาในขั้นตอนการจัดซื้อจัดจ้างและการดูแลรักษาครุภัณฑ์ ซึ่งเป็นภาระของเจ้าหน้าที่ผู้ดูแลระบบ และยากต่อการบริหารจัดการ นั้นดังนั้น จึงเห็นควรใช้วิธีการเช่าใช้แทนการซื้อระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชุดใหม่เพื่อให้สำนัก กสทช. มีความปลอดภัย มีประสิทธิภาพ ในการใช้งานระบบเครือข่าย และ ระบบคอมพิวเตอร์เสมือน

๒. วัตถุประสงค์

เพื่อเช่าใช้ระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูง จำนวน ๑ ระบบ สำหรับติดตั้งใช้งานที่สำนักงาน กสทช. โดยมีระยะเวลาในการเช่า ๓๖ เดือน

๓. คุณสมบัติผู้ยื่นข้อเสนอ

๓.๑ มีความสามารถตามกฎหมาย

๓.๒ ไม่เป็นบุคคลล้มละลาย

๓.๓ ไม่อยู่ในระหว่างการเลิกกิจการ

๓.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๓.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๓.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๓.๗ ไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม

๓.๘ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ให้เช่าได้มีคำสั่งให้สละสิทธิ์ความคุ้มกันเช่นว่านั้น

๓.๙ ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e - GP) ของกรมบัญชีกลาง

๓.๑๐ ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายหรือผู้ให้เช่าอุปกรณ์ระบบตรวจจับและป้องกันการบุกรุกเครือข่าย จากบริษัทผู้ผลิต หรือสาขาของบริษัทผู้ผลิตประจำประเทศไทย

๔. รายละเอียดคุณลักษณะเฉพาะ

๔.๑ ข้อกำหนดทั่วไป

๔.๑.๑ ระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงประกอบด้วย

๔.๑.๑.๑ อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) จำนวน ๒ ชุด

๔.๑.๑.๒ อุปกรณ์บริหารจัดการระบบป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) จำนวน ๑ ชุด

๔.๑.๑.๓ อุปกรณ์ตรวจจับและวิเคราะห์ภัยคุกคามชั้นสูง (Advanced Persistent Threats) จำนวน ๑ ชุด

๔.๑.๑.๔ ระบบศูนย์กลางในการมองเห็นและบริหารจัดการแบบรวมศูนย์ (Centralized Visibility and Control) จำนวน ๑ ระบบ

๔.๑.๒ ผู้ให้เช่าต้องสำรวจ วิเคราะห์ และออกแบบ พร้อมทั้งส่งแผนการดำเนินงานการติดตั้ง โดยต้องได้รับความเห็นชอบจากคณะกรรมการตรวจรับเพื่อให้เห็นชอบก่อนดำเนินการติดตั้ง

๔.๑.๓ ผู้ยื่นข้อเสนอต้องมีหนังสือรับรองต้นฉบับจากบริษัทผู้ผลิต หรือบริษัทที่เป็นสาขาของผู้ผลิต สำหรับ ผลิตภัณฑ์ Hardware หรือ Software ที่เสนอ โดยมีเนื้อหาระบุว่าเป็นของใหม่ไม่เคยใช้งานมาก่อน อยู่ในสายการผลิตมีการสนับสนุนด้านเทคนิคตลอดระยะเวลาการเช่า

๔.๑.๔ ผู้ให้เช่าจะต้องส่งมอบระบบ พร้อมเอกสารประกอบการติดตั้งอย่างน้อยดังนี้

- คู่มือมาตรฐานของผู้ผลิต (Hardware และ Software) ทั้งหมดตามที่เสนอ
- เอกสารแสดงการกำหนดค่าติดตั้งต่าง ๆ (Configuration) ผังการเชื่อมต่ออุปกรณ์ต่าง ๆ กับเครือข่าย (Network) ของอุปกรณ์ที่เสนอทั้งหมด
- เอกสารแสดงการกำหนดค่า Configuration ของระบบทั้งหมดตามที่เสนอ

๔.๑.๕ ผู้ให้เช่าจะต้องดำเนินการจัดฝึกอบรมด้านเทคนิค ให้เจ้าหน้าที่ผู้ดูแลระบบสำนักงาน กสทช. จำนวนอย่างน้อย ๓ คน

๔.๒ ข้อกำหนดทางด้านเทคนิค

๔.๒.๑ อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) จำนวน ๒ ชุด มีคุณสมบัติอย่างน้อยดังนี้

๔.๒.๑.๑ ต้องเป็น Hardware ที่ออกแบบมาเพื่อทำหน้าที่ป้องกันการบุกรุกทางเครือข่าย Next Generation Intrusion Prevention (NGIPS) หรือ Data Center Intrusion Prevention (DCIPS) โดยเฉพาะ ไม่เป็นลักษณะ Unified Threat Management (UTM) หรือ Next Generation Firewall (NGFW)

๔.๒.๑.๒ ต้องมี IPS Inspection Throughput ไม่น้อยกว่า ๕ Gbps และรองรับการขยายความเร็วในการตรวจจับได้ไม่น้อยกว่า ๔๐ Gbps ในหนึ่งระบบ โดยไม่ต้องเปลี่ยนอุปกรณ์ โดยสามารถอ้างอิงจาก Website หรือ เอกสารจากเจ้าของผลิตภัณฑ์

๔.๒.๑.๓ สามารถรองรับการเชื่อมต่อ Current Sessions ไม่น้อยกว่า ๑๒๐,๐๐๐,๐๐๐ Sessions ในหนึ่งระบบ โดยจะเป็นอุปกรณ์เพียงตัวเดียว หรือ ทำ stacking หรือเสนออุปกรณ์ กระจายโหลดเพิ่มเติมเพื่อให้สามารถรับโหลดดังกล่าวได้ โดยสามารถอ้างอิงจาก Website หรือเอกสารจากเจ้าของผลิตภัณฑ์

๔.๒.๑.๔ สามารถรองรับการเชื่อมต่อ New Connections ได้ไม่น้อยกว่า ๖๕๐,๐๐๐ Connections per second ในหนึ่งระบบ โดยสามารถอ้างอิงจาก Website หรือ เอกสารจากเจ้าของผลิตภัณฑ์

๔.๒.๑.๕ สามรถรองรับการทำ SSL Inspection Throughput ได้ไม่น้อยกว่า ๒ Gbps ในหนึ่งระบบ โดยสามารถอ้างอิงจาก Website หรือ เอกสารจากเจ้าของผลิตภัณฑ์

๔.๒.๑.๖ สามารถรับการเชื่อมต่อ (Network Connectivity) ได้อย่างน้อย ๑๐ Segments โดยเป็นประเภท interface ดังต่อไปนี้

(๑) มี interface แบบ ๑GE Copper ไม่น้อยกว่า ๖ Segments หรือ ๑๒ พอร์ต

(๒) มี Interface แบบ ๑๐GE SFP+ Multi-Mode (SR) ไม่น้อยกว่า ๔ Segments หรือ ๘ พอร์ต พร้อม Transceiver สำหรับการเชื่อมต่อ

๔.๒.๑.๗ ผลิตภัณฑ์ที่นำเสนอจะไม่ทำให้ระบบเกิดการหน่วง (Latency) หรือยอมให้เกิดได้ ไม่เกิน ๕๐ µS (microseconds) โดยสามารถอ้างอิงจาก Website หรือ เอกสารจากเจ้าของผลิตภัณฑ์ได้

๔.๒.๑.๘ ต้องมี Management Port แบบ out-of-band ๑๐/๑๐๐/๑๐๐๐ RJ-๔๕ จำนวนอย่างน้อย ๑ พอร์ต

๔.๒.๑.๙ สามารถตรวจจับวิธีการบุกรุกและป้องกันเครือข่ายได้ดังต่อไปนี้เป็นอย่างน้อย Exploits, Identity Theft, Spyware, Virus, Vulnerabilities, Network Equipment (Malicious attacks through printers, modems, routers and integrated phone systems) , Traffic Normalization (improper or malformed traffic) , Instant Messaging, Peer-to-Peer (P๒P), Streaming Media และ DDoS ได้เป็นอย่างน้อย

๔.๒.๑.๑๐ สามารถในการควบคุมข้อมูลที่น่าสงสัยจาก IP Address, Domains หรือ URL โดยการใช้ข้อมูลจาก Reputation Database ได้

๔.๒.๑.๑๑ สามารถในการจัดการทราฟฟิคจาก geographic region หรือ country ได้

๔.๒.๑.๑๒ ต้องมีขั้นตอนวิธีในการตรวจจับ DNS requests จาก Infected Hosts เพื่อป้องกันระบบจาก Known Malware Families และ Suspicious Domain Names ที่สร้างจาก Unknown Malware Families

๔.๒.๑.๑๓ สามารถในการป้องกัน Known, Unknown และ Undisclosed vulnerabilities โดยการใช้ข้อมูลจาก Threat Intelligence หรือ Researchers จากเจ้าของผลิตภัณฑ์ได้

๔.๒.๑.๑๔ สามารถทำงานร่วมกับระบบตรวจจับและวิเคราะห์ภัยคุกคามขั้นสูง (Advanced Persistent Threats) ที่นำเสนอในโครงการได้

๔.๒.๑.๑๕ ต้องมี Power Supply แบบ Redundant Hot-Swappable จำนวน ๒ หน่วย

๔.๒.๑.๑๖ สามารถใช้งานตามมาตรฐาน IPv๖ และ GRE ได้

๔.๒.๑.๑๗ อุปกรณ์ที่นำเสนอจะต้องได้รับการรับรองความปลอดภัยในการใช้งานจาก EN, UL, FCC, VCCI และ CSA เป็นอย่างน้อย

๔.๒.๑.๑๘ อุปกรณ์ต้องสามารถติดตั้งในตู้ RACK ขนาดมาตรฐาน ๑๙ นิ้วได้

๔.๒.๒ อุปกรณ์บริหารจัดการระบบป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) จำนวน ๑ ชุด มีคุณสมบัติอย่างน้อยดังนี้

๔.๒.๒.๑ ต้องเป็น Hardware ที่ออกแบบมาสำหรับบริหารจัดการระบบป้องกันและตรวจจับการบุกรุกที่นำเสนอแบบรวมศูนย์ (Centralized Management) เท่านั้น

๔.๒.๒.๒ มีหน้า Dashboard ที่แสดงข้อมูลเหล่านี้เป็นอย่างน้อย

(๑) Health and Status เพื่อให้ข้อมูล Memory และ CPU usage รวมทั้งสถานะของ Managed Devices

(๒) Task Status เพื่อให้ข้อมูลของการกระจาย Profile, Reputation และ Software Version ปัจจุบันของ IPS

(๓) Inspection Event เพื่อแสดงข้อมูลเกี่ยวกับ Events ที่เกิดขึ้น และ Top Events ตาม IP หรือ Geographic location

(๔) Security เพื่อให้ข้อมูลของจำนวนการ Attacks, Top Attack Destinations (IP และ Geography) และ Top Attack Sources (IP และ Geography) ได้อย่างน้อย

(๕) Reputation เพื่อให้ข้อมูลของ Top Reputation DNS Names และ Top Reputation IP Addresses

(๖) User เพื่อให้ข้อมูลของ Top App Users และ Top Attack Users รวมทั้งสามารถทำ Customized Dashboard ได้เป็นอย่างน้อย

๔.๒.๒.๓ สามารถจัดทำ Reports ดังต่อไปนี้ได้เป็นอย่างน้อย

(๑) All attacks, Top attacks, Top attacks by country, Top destinations, Top IPS VLANs with attacks, Top sources และ Top users

(๒) All applications, Top applications, Top attacks by country และ Top P๒P peers

(๓) All DNS Requestors, All Reputation DNS Names, All Reputation IP Addresses, Top DNS Requestors, Top Reputation by Country, Top Reputation DNS Names และ Top Reputation IP Addresses

(๔) Rate Limit Reports, DDoS Reports และ Executive Reports

๔.๒.๒.๔ มีความยืดหยุ่นในการบริหารจัดการ Network Security Policy ไปยัง IPS devices ได้

๔.๒.๒.๕ สามารถส่งข้อมูลแจ้งเตือนไปยัง Syslog Server, Email และ SNMPv๒ ได้เป็นอย่างน้อย

๔.๒.๒.๖ สามารถรองรับการทำงานร่วมกับ Third-party Vulnerability Assessments ได้แก่ Rapid๗, Qualys และ Tenable เพื่อนำข้อมูล CVEs ที่ได้ไปใช้ในการปรับ IPS Security Policy ให้ป้องกัน Known Vulnerabilities ในระบบ Network ได้

๔.๒.๒.๗ สามารถบริหารจัดการอุปกรณ์ป้องกันและตรวจจับการบุกรุกได้ ไม่น้อยกว่า ๒๕ ชุด

๔.๒.๒.๘ สามารถรับเหตุการณ์ (Events) ได้ไม่น้อยกว่า ๒๐๐ Million Historical Events โดยสามารถอ้างอิงจาก Website หรือ เอกสารจากเจ้าของผลิตภัณฑ์ได้

๔.๒.๒.๙ สามารถบริหารจัดการผ่าน Web-based interface และ Command Line Interface (CLI) ได้

๔.๒.๒.๑๐ มี Power Supply แบบ Redundant หรือ Hot Swappable เป็นอย่างน้อย

๔.๒.๒.๑๑ อุปกรณ์ต้องสามารถติดตั้งในตู้ RACK ขนาดมาตรฐาน ๑๙ นิ้วได้

๔.๒.๓ อุปกรณ์ตรวจจับและวิเคราะห์ภัยคุกคามชั้นสูง (Advanced Persistent Threats) จำนวน ๑ ระบบ มีคุณสมบัติอย่างน้อยดังนี้

๔.๒.๓.๑ สามารถตรวจจับและป้องกันภัยคุกคามดังต่อไปนี้ได้ เป็นอย่างน้อย

(๑) Targeted Attacks และ Advanced Threats

(๒) Targeted และ Known Ransomware Attacks

(๓) Zero-day Malware และ Document Exploits

(๔) Attacker Behavior และ Other Network Activity

(๕) Web Threats, including Exploits และ Drive-by Downloads

(๖) Phishing, Spear Phishing, และ Other Email Threats

(๗) Data Exfiltration

(๘) Bots, Trojans, Worms, Keyloggers

(๙) Disruptive Applications

๔.๒.๓.๒ สามารถในการตรวจสอบภัยคุกคามขั้นสูงด้วยเทคโนโลยีอย่างน้อย ดังนี้

(๑) Custom Sandbox Analysis

(๒) Broad File Analysis Range

(๓) Document Exploit Detection

(๔) URL analysis Pattern

(๕) Detect Zero-day exploits

(๖) Web services API and manual submission

(๗) Discover Ransomware through reputation-based analysis

(๘) Superior Evasion Resistance

๔.๒.๓.๓ สามารถรับตัวอย่างภัยคุกคามที่ต้องสงสัยจำพวก URL จาก Intrusion Prevention System ที่นำเสนอในโครงการเพื่อทำการวิเคราะห์บนระบบ sandbox หลังจากนั้นสามารถออกผลการวิเคราะห์กลับมาเพื่อระบุเครื่องที่มีความเสี่ยง รวมทั้งรองรับการร่วมกับระบบที่มีอยู่เดิมดังนี้ได้

(๑) Palo Alto Firewall หรือ CheckPoint

(๒) BlueCoat

๔.๒.๓.๔ สามารถในการ monitors ทุกทราฟฟิคที่ผ่าน Physical และ Virtual network Segments โดยรองรับมากกว่า ๑๐๐ Network Protocols เพื่อช่วยตรวจสอบ Target Attacks, Advanced Threats และ Ransomware จากทั้ง Inbound, Outbound Network Traffic, Lateral Movement และ C&C ได้

๔.๒.๓.๕ สามารถในการตรวจจับ APT and Targeted Attacks รวมทั้งการระบุ Malicious Content, Communications and Behavior ที่สื่อถึง Advanced Malware ผ่านทุกๆขั้นตอนของการโจมตีดังต่อไปนี้ได้

(๑) Intelligence Gathering

(๒) Point of Entry

(๓) C&C Communication

(๔) Lateral Movement

(๕) Assets/Data Discovery

(๖) Data Exfiltration

(๗) Unknown Attack Phase

๔.๒.๓.๖ สามารถทำงานร่วมกับระบบป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) ที่นำเสนอในโครงการได้ ด้วยการส่งข้อมูลที่ต้องสงสัยเกี่ยวกับ IP Addresses และ Domain Names ให้กับระบบ ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) เพื่อ Block ได้

๔.๒.๓.๗ สามารถทำ Packet Capture (pcap) เพื่อทำการตรวจสอบระหว่างการโจมตี และหลังการโจมตีได้

๔.๒.๓.๘ สามารถเลือกสร้างระบบวิเคราะห์จำลองเสมือน (Custom Virtual Analyzer หรือ Custom Sandbox) บนระบบปฏิบัติ Windows XP, Windows ๗, Windows ๘/๘.๑, Windows ๑๐, Windows Server ๒๐๐๓, Windows Server ๒๐๐๘, Windows Server ๒๐๑๒, และ Windows Server ๒๐๑๖ รวมทั้งรองรับการทำ Sandbox สำหรับ MacOS เพื่อเพิ่มความปลอดภัยให้ระบบมากยิ่งขึ้น

๔.๒.๓.๙ Virtual Analyzer ในระบบที่นำเสนอสามารถทำ Static และ Dynamic Analysis เพื่อวิเคราะห์ลักษณะเฉพาะตามหมวดหมู่ดังนี้ได้

(๑) Anti-Security และ Self-Preservation
(๒) Auto start หรือ Other System Configuration
(๓) Deception และ Social Engineering
(๔) File Drop, Download, Sharing, หรือ Replication
(๕) Hijack, Redirection, หรือ Data Theft
(๖) Malformed, Defective หรือ Known Malware Traits
(๗) Process, Service หรือ Memory Object Change
(๘) Rootkit, Cloaking
(๙) Suspicious Network หรือ Messaging Activity

๔.๒.๓.๑๐ สามารถรองรับการการทำ Sandbox ได้สูงสุดที่ ๖๐ Instances

๔.๒.๓.๑๑ สามารถแสดงข้อมูลในการตรวจจับดังต่อไปนี้ได้เป็นอย่างน้อย

(๑) Activity detected
(๒) Attack phase
(๓) Detection name
(๔) Detection rule ID
(๕) Detection severity
(๖) Detection type
(๗) Event class
(๘) Notable Object
(๙) Protocol
(๑๐) Reference
(๑๑) Targeted attack campaign
(๑๒) Targeted attack related
(๑๓) Threat
(๑๔) Threat description
(๑๕) Timestamp
(๑๖) URL category
(๑๗) Virtual Analyzer risk level

๔.๒.๓.๑๒ สามารถรองรับการตรวจหาภัยคุกคามใน Protocol SMB, DHCP, DNS, File Transfer, FTP, HTTP, ICMP, IMAP๔, POP๓, MODBUS, RDP, SCADA, TELNET, SMTP, MSSQL, MYSQL, ORACLE, POSTGRES, SQL, RTMP, RTSP, TCP, TFTP, UDP, SIP๒, IGMP, IP, MMS, SNMP และ SSH ได้เป็นอย่างน้อย

๔.๒.๓.๑๓ สามารถสร้างรายงาน (Report) ได้ ทั้งแบบ On-Demand และ Schedules โดยออกมาในรูปแบบ PDF ได้เป็นอย่างน้อย รวมทั้งสามารถส่งเป็น email ออกไปให้กับผู้ดูแลระบบได้

๔.๒.๓.๑๔ สามารถสร้างรายการ Executive Report, Host Severity Report, Summary Report และ Threat Detection Report ได้เป็นอย่างน้อย

๔.๒.๓.๑๕ มีดิสก์สำหรับเก็บข้อมูลรวมกันไม่น้อยกว่า ๔ TB

๔.๒.๓.๑๖ สามารถรับตัวอย่างภัยคุกคามที่ต้องสงสัยจำพวก file จากซอฟต์แวร์ด้านความปลอดภัยสำหรับเครื่องแม่ข่าย (Server Security Software) ที่มีอยู่เดิมได้

๔.๒.๓.๑๗ ต้องอยู่ในกลุ่ม Recommended ของ NSS LABS report ในส่วนของ Breach Detection Systems (BDS) Security Value Map ปี ๒๐๑๗ และ ๒๐๑๘ เท่านั้น และเจ้าของผลิตภัณฑ์ต้องมีสาขาในประเทศไทยเพื่อรองรับบริการหลังการเช่า

๔.๒.๔ ระบบศูนย์กลางในการมองเห็นและบริหารจัดการแบบรวมศูนย์ (Centralized Visibility and Control) จำนวน ๑ ระบบ มีคุณลักษณะอย่างน้อย ดังนี้

๔.๒.๔.๑ เป็นศูนย์กลางในการบริหารจัดการโดยสามารถทำงานร่วมกับระบบป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) และระบบระบบตรวจจับและวิเคราะห์ภัยคุกคามขั้นสูง (Advanced Persistent Threats) ที่นำเสนอในโครงการผ่านหน้า web-based console รวมทั้งซอฟต์แวร์ด้านความปลอดภัยสำหรับเครื่องแม่ข่าย (Server Security Software)ได้

๔.๒.๔.๒ มีหน้า Dashboard ที่สามารถแสดงข้อมูลดังต่อไปนี้ได้

(๑) Critical Threats
(๒) Resolved Events
(๓) Users with Threats
(๔) Endpoints with Threats
(๕) Top Threats
(๖) Product Connection Status
(๗) Product Component Status
(๘) Product Application Compliance
(๙) Ransomware Prevention
(๑๐)Threat Statistics
(๑๑)Threat Detection Results
(๑๒)Policy Violation Detections
(๑๓)C&C Callback Events

๔.๒.๔.๓ สามารถช่วยในการตรวจจับ, วิเคราะห์ และโต้ตอบภัยคุกคามแบบ targeted attacks และ advanced threats ด้วยความสามารถดังต่อไปนี้

(๑) Security Threat Monitoring
(๒) Suspicious Object List Synchronization
(๓) Suspicious Object Management
(๔) Suspicious Object Scan Actions
(๕) Impact Assessment
(๖) Endpoint Isolation
(๗) IOC Management

๔.๒.๔.๔ ต้องสามารถแสดงสถานะ (status) ของ command ที่ส่งไปยัง managed products ว่าสำเร็จหรือไม่ได้

๔.๒.๔.๕ สามารถสร้าง User Account ใหม่ หรือรับข้อมูลจาก Active Directory รวมทั้งกำหนด User Role ในการใช้งานเพื่อควบคุมการเข้าถึงและใช้งานได้

๕. ระยะเวลาส่งมอบงาน

ผู้ให้เช่าจะต้องส่งมอบและติดตั้งระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูง สำนักงาน กสทช. จำนวน ๑ ระบบ ภายใน ๕ เดือน โดยนับถัดจากวันลงนามในสัญญาและเมื่อตรวจรับเรียบร้อยจึงเริ่มดำเนินการเช่าเป็นระยะเวลา ๓๖ เดือน โดยผู้ให้เช่าต้องส่งมอบรายงานการเช่าระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงสำนักงาน กสทช. จำนวน ๑ ระบบ เป็นงวดๆ ละ ๑ เดือน ภายใน ๑๕ วัน ทำการของเดือนถัดไป

๖. งบประมาณ

งบประมาณทั้งสิ้นจำนวน ๒๔,๔๖๒,๐๐๐.- บาท (ยี่สิบสี่ล้านสี่แสนหกหมื่นสองพันบาทถ้วน) ซึ่งรวมภาษีมูลค่าเพิ่มแล้ว แบ่งจ่ายและผูกพันงบประมาณ ดังนี้.-

ตั้งงบประมาณปี ๒๕๖๓	จำนวน ๔,๐๗๗,๐๐๐	บาท
ผูกพันงบประมาณปี ๒๕๖๔	จำนวน ๘,๑๕๔,๐๐๐	บาท
ผูกพันงบประมาณปี ๒๕๖๕	จำนวน ๘,๑๕๔,๐๐๐	บาท
ผูกพันงบประมาณปี ๒๕๖๖	จำนวน ๔,๐๗๗,๐๐๐	บาท

โดยเบิกจ่ายจากงบประมาณรายจ่าย ประจำปี ๒๕๖๓ และผูกพันสัญญาปี ๒๕๖๔-๒๕๖๖ สำนักเทคโนโลยีสารสนเทศ หมวดค่าใช้จ่ายในการจัดการและบริหารองค์กร รายจ่ายเกี่ยวกับการจัดการและบริหารองค์กร

๗. หลักเกณฑ์การพิจารณาการคัดเลือก

สำนักงาน กสทช. จะพิจารณาคัดเลือกข้อเสนอโดยใช้เกณฑ์ราคา

๘. เงื่อนไขการชำระเงิน

สำนักงาน กสทช. จะจ่ายค่าเช่าระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูง สำนักงาน กสทช. ให้แก่ผู้ให้บริการเป็นงวด งวดละเท่ากัน รวม ๓๖ งวด เมื่อผู้ให้บริการได้ส่งรายงานสรุปผลการจ้างเช่าระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูง สำนักงาน กสทช. ตามข้อ ๖.๒ และคณะกรรมการตรวจรับพัสดุได้ตรวจสอบรับรองครบถ้วนถูกต้องเรียบร้อยแล้ว

๙. เงื่อนไขเมื่อสิ้นสุดสัญญาเช่า

ผู้ให้เช่าจะต้องขนย้ายอุปกรณ์ระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงกลับคืนภายใน ๓๐ วัน นับถัดจากวันที่สำนักงาน กสทช. แจ้งให้ทราบหากพ้นกำหนด สำนักงาน กสทช. จะไม่รับผิดชอบความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์ระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงดังกล่าว และผู้ให้เช่าจะต้องรับผิดชอบค่าใช้จ่ายในการขนย้ายด้วย

๑๐. การรับประกันผลงานและค่าปรับ

๑๐.๑ การบริการ

๑๐.๑.๑ ผู้ให้เช่ามีหน้าที่บำรุงรักษาและซ่อมแซมแก้ไขระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงให้รวมถึงการบำรุงรักษาเพื่อป้องกันความชำรุดเสียหาย (Preventive Maintenance) ตลอดระยะเวลาดำเนินงาน และต้องทำการซ่อมแซมแก้ไขและเปลี่ยนสิ่งที่จำเป็นทุกประการ (Corrective Maintenance) เพื่อให้ระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงอยู่ในสภาพใช้งานได้ดีตามปกติโดยไม่คิดค่าใช้จ่ายใดๆ เพิ่มเติมทั้งสิ้น

๑๐.๑.๒ ผู้ให้เช่าจะต้องจัดให้ช่างผู้มีความรู้ความชำนาญและฝีมือดีมาตรวจสอบบำรุงรักษาคอมพิวเตอร์ (Preventive Maintenance) อย่างน้อยเดือนละ ๑ ครั้ง ในกรณีคอมพิวเตอร์ขัดข้องใช้การไม่ได้ตามปกติผู้รับจ้างจะต้องจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพใช้การได้ดีดังเดิม (Corrective Maintenance) โดยต้องเริ่มจัดการซ่อมแซมแก้ไขภายในระยะเวลาที่กำหนดตามข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) นับตั้งแต่เวลาที่ได้รับแจ้งจากผู้ว่าจ้างหรือผู้ที่ได้รับมอบหมายจากผู้ว่าจ้าง โดยจะแจ้งให้ผู้รับจ้างหรือผู้ที่ได้รับมอบหมายจากผู้รับจ้างทราบทางวาจา ทางโทรสาร หรือทางไปรษณีย์อิเล็กทรอนิกส์ (e-mail) หรือทางโทรศัพท์ ไม่ว่าวิธีใดวิธีหนึ่งให้ถือเป็นการแจ้งโดยชอบแล้ว และผู้รับจ้างจะต้องซ่อมแซมแก้ไข หรือเปลี่ยนสิ่งที่จำเป็นให้เสร็จเรียบร้อยภายในระยะเวลาที่กำหนดตามข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) นับแต่เวลาที่ได้รับแจ้งจากผู้ว่าจ้างดังกล่าว

๑๐.๑.๓ ผู้ให้เช่าต้องปฏิบัติตามข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) บำรุงรักษา ซ่อมแซม แก้ไข ที่มีรายละเอียดดังนี้

ระดับความรุนแรงของปัญหา	สถานการณ์	ช่องทางการให้บริการ	ระยะเวลาการตอบสนองและติดตามการแก้ไขปัญหา
ระดับ ๑ : สูง	ระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูง ไม่สามารถใช้งานได้	บริการแก้ไขปัญหาแบบ Remote Access /Onsite	ตอบสนองภายใน ๔ ชั่วโมง และแก้ปัญหาให้แล้วเสร็จภายใน ๑๒ ชั่วโมง
ระดับ ๒ : ปานกลาง	บางส่วนไม่สามารถใช้งานได้ ซึ่งไม่กระทบกับการทำงานของระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูง	ณ. จุดรับการติดต่อประสานงาน หรือ Remote Access	ตอบสนองภายใน ๘ ชั่วโมง และแก้ปัญหาให้แล้วเสร็จภายใน ๑๘ ชั่วโมง
ระดับ ๓ : ต่ำ	คำแนะนำเกี่ยวกับการใช้งานระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูง โดยเครื่องดังกล่าว ยังใช้งานได้ตามปกติ	ณ. จุดรับการติดต่อประสานงาน	ตอบสนองและแจ้งผลการแก้ไขตามกำหนดที่ตกลงกับผู้แจ้งฯ

ทั้งนี้ หากอุปกรณ์ระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงที่ดำเนินการแก้ไขแล้วไม่สามารถใช้งานได้อย่างมีประสิทธิภาพ ผู้ให้เช่าต้องดำเนินการจัดหาอุปกรณ์ระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูง ใหม่ที่มีความสามารถเท่าเดิมหรือดีกว่าของเดิมมาเปลี่ยนให้ผู้เช่าใหม่

๑๐.๑.๔ หากผู้ให้เช่าไม่ดำเนินการดังกล่าว ผู้เช่ามีสิทธิจ้างบุคคลภายนอกทำการซ่อมแซมแก้ไข โดยผู้ให้เช่าจะต้องออกค่าใช้จ่ายในการจ้างบุคคลภายนอกซ่อมแซมแก้ไขแทนผู้เช่าทั้งสิ้นการจ้างบริการบำรุงรักษาและซ่อมแซมแก้ไขระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงตามสัญญานี้ ไม่รวมถึงการเปลี่ยนแปลงลักษณะเฉพาะของระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงหรือส่วนประกอบที่ติดตั้งเพิ่มเติมภายหลังที่สัญญานี้มีผลบังคับและความเสียหายของระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงซึ่งเกิดจากเหตุสุดวิสัยหรือเกิดจากความผิดของผู้เช่า

๑๐.๒ การรับประกันผลงาน

๑๐.๒.๑ ผู้ให้เช่าตกลงบำรุงรักษาและซ่อมแซมแก้ไขระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงตามสัญญานี้ให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอ โดยให้มีเวลาระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงขัดข้องรวมตามเกณฑ์การคำนวณเวลาขัดข้อง ไม่เกินเดือนละ ๓๖ ชั่วโมง หรือร้อยละ ๕ ของเวลาใช้งานทั้งหมดของระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงของเดือนนั้น แล้วแต่ตัวเลขใดจะมากกว่ากัน มิฉะนั้นผู้รับจ้างต้องยอมให้ผู้เช่าคิดค่าปรับเป็นรายชั่วโมงในอัตราชั่วโมงละ ๐.๐๓๕% ของค่าเช่าตามสัญญา ในช่วงเวลาที่ไม่สามารถใช้ระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงได้ในส่วนที่เกินกว่ากำหนดเวลาขัดข้องข้างต้น

๑๐.๒.๒ เกณฑ์การคำนวณเวลาขัดข้องของระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงตามข้อ ๑๐.๑ ให้เป็นไปดังนี้

(๑) กรณีที่ระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงเกิดขัดข้องพร้อมกันหลายหน่วย ให้นับเวลาขัดข้องของหน่วยที่มีตัวถ่วงมากที่สุดเพียงหน่วยเดียว

(๒) กรณีความเสียหายอันสืบเนื่องมาจากความขัดข้องของอุปกรณ์ระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงแตกต่างกัน เวลาที่ใช้ในการคำนวณค่าปรับจะเท่ากับเวลาขัดข้องของอุปกรณ์ระบบตรวเจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงหน่วยนั้นคูณด้วยตัวถ่วงซึ่งมีค่าต่าง ๆ ตามเอกสารแนบท้ายขอบเขตของงาน

๑๐.๓ ค่าปรับ

๑๐.๓.๑ ในกรณีที่ผู้ให้เช่าไม่สามารถติดตั้งอุปกรณ์ของระบบที่เช่าภายในระยะเวลาที่กำหนด ผู้ให้เช่าจะต้องชำระค่าปรับให้ สำนักงาน กสทช. เป็นรายวันในอัตราร้อยละ ๐.๒ (๐.๒%) ของอุปกรณ์ที่ยังไม่ได้ส่งมอบ จนถึงวันที่ผู้ให้เช่าได้ส่งมอบงานให้สำนักงาน กสทช. เป็นที่เรียบร้อยแล้ว

๑๐.๓.๒ ในกรณีที่ผู้ให้เช่าไม่เข้ามาซ่อมแซมแก้ไขภายในเวลาที่กำหนด หรือไม่สามารถดำเนินการซ่อมแซมแก้ไขหรือไม่สามารถจัดหาอุปกรณ์ใหม่ที่มีคุณสมบัติทัดเทียมกันหรือดีกว่ามาเปลี่ยนให้ใช้งานได้ภายในเวลาที่กำหนดไว้ตามข้อ

๑๐.๑ (๒) ผู้ให้เช่ายินยอมให้คิดค่าปรับเป็นรายชั่วโมง (เศษของชั่วโมงให้นับเป็น ๑ (หนึ่ง) ชั่วโมง) ในอัตราร้อยละ ๐.๑ นับจากเวลาที่ครบกำหนดจนถึงเวลาที่ผู้ผู้ให้เช่าได้เริ่มการซ่อมแซมแก้ไข หรือจนถึงเวลาที่ผู้ให้เช่าดำเนินการซ่อมแซมแก้ไขแล้วเสร็จแล้วแต่กรณี

๑๐.๓.๓ ในกรณีที่ผู้ให้เช่าไม่ชดใช้อุปกรณ์ระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูงที่ได้รับความเสียหายตามข้อ ๑๐.๑ (๔) ต้องยินยอมให้คิดค่าปรับเป็นรายวันในอัตราร้อยละ ๐.๑ ตามสัญญานับถัดจากวันที่ครบกำหนด จนถึงวันที่นำอุปกรณ์ชุดใหม่มาส่งมอบครบถ้วน

๑๐.๓.๔ หากผู้ให้เช่าไม่เข้าทำการบำรุงรักษาเพื่อป้องกัน (Preventive Maintenance : PM) ตามรอบระยะเวลาที่กำหนด ต้องยินยอมให้คิดค่าปรับในอัตราร้อยละ ๐.๑๐ ของเช่าตามสัญญา และเนื่องจากการไม่เข้าบำรุงรักษานั้นไม่สามารถชดเชยในรอบระยะเวลาถัดไปได้ ถือเป็นการกระทำที่ผิดสัญญา ผู้เช่าจะหักค่าเช่าที่ต้องจ่ายในงวดนั้นลงตามส่วน รวมทั้งค่าเสียหายอันเกิดจากการไม่ทำการบำรุงรักษานั้น (ถ้ามี) นอกจากจากค่าปรับดังกล่าวอีกด้วย

เอกสารแนบ

การกำหนดตัวถ่วงของระบบตรวจจับและป้องกันการบุกรุกเครือข่ายชั้นสูง

สำนักงาน กสทช. จำนวน ๑ ระบบ

ลำดับที่	รายการ	น้ำหนักตัวถ่วง
๑.	อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) จำนวน ๒ ชุด	๑
๒.	อุปกรณ์บริหารจัดการระบบป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) จำนวน ๑ ชุด	๑
๓.	อุปกรณ์ตรวจจับและวิเคราะห์ภัยคุกคามชั้นสูง (Advanced Persistent Threats) จำนวน ๑ ชุด	๑
๔.	ระบบศูนย์กลางในการมองเห็นและบริหารจัดการแบบรวมศูนย์ (Centralized Visibility and Control) จำนวน ๑ ระบบ	๑