ขอบเขตของงาน (Term of Reference)
ระบบตรวจสอบและวิเคราะห์ภัยคุกคามเครื่องคอมพิวเตอร์ลูกข่าย
(Endpoint Detection and Respond) สำนักงาน กสทช. จำนวน ๑ ระบบ

๑. หลักการและเหตุผล

ปัจจุบันสำนักงาน กสทช. มีการใช้เทคโนโลยีสารสนเทศในการสนับสนุนการดำเนินงานที่เพิ่มขึ้น ทั้งยังมีการพัฒนาให้ทันสมัยและเป็นปัจจุบันอยู่ตลอดเวลา เมื่อมีการพัฒนาระบบให้ตอบสนองต่อความต้องการใหม่ๆ ต้องปรับตัวให้เท่าทันภัยคุกคามทางด้านเทคโนโลยีสารสนเทศที่นับวันมีแนวโน้มเพิ่มขึ้น มีวิวัฒนาการที่ซับซ้อนขึ้น ส่งผลกระทบที่มีความรุนแรงและเป็นวงกว้างมากขึ้น ดังเช่น เหตุการณ์ภัยคุกคามทางด้านเทคโนโลยีสารสนเทศที่เกิดขึ้นทั่วโลกที่มุ่งโจมตีมาที่เครื่องลูกข่ายโดยตรง ไม่ว่าจะกรณีเปิดลิงค์ Phishing หรือการเข้าเว็บไซต์ที่ถูกโจมตีมัลแวร์ฝังด้วยคำสั่ง Cross-site Script (XSS) แล้วการดาวน์โหลดไฟล์มัลแวร์ที่ไม่เคยพบเห็นมาก่อนหรือไม่มีบนฐานข้อมูลบนโปรแกรมป้องกันไวรัสเข้ามาโดยอัตโนมัติ การกระทำดังกล่าวดำเนินการผ่านการเชื่อมต่อที่มีการเข้ารหัสลับเพื่อเป็นการหลีกเลี่ยงหรือทำให้ระบบรักษาความปลอดภัยบนเครื่องลูกข่าย (Trend Micro APEX One) และระบบตรวจจับป้องกันการบุกรุก (Trend Micro Tipping Point/DDI/DDAN) ที่สำนักงาน กสทช. ใช้งานอยู่ในปัจจุบันไม่สามารถตรวจจับได้หากมีหลุดรอดออกไป เนื่องจากยังขาดฟังก์ชั่นในการตรวจสอบและวิเคราะห์ภัยคุกคาม ทำให้ไม่สามารถตรวจสอบป้องกันเหตุการณ์ข้างต้นได้ทันท่วงที และยากต่อการสืบสวนหาสาเหตุที่แท้จริงของการโจมตีหรือระบุตำแหน่งเครื่องลูกข่ายที่เป็นเครื่องต้นตอในการแพร่กระจายมัลแวร์ไปยังเครื่องคอมพิวเตอร์อื่นๆ ในสำนักงาน กสทช.

ระบบตรวจสอบและวิเคราะห์ภัยคุกคามเครื่องคอมพิวเตอร์ลูกข่าย (Endpoint Detection and Respond) เป็นระบบที่ช่วยป้องกันการโจมตีจากมัลแวร์ที่ไม่เคยพบเห็นมาก่อน โดยใช้ข้อมูลการวิเคราะห์อย่างละเอียดเกี่ยวกับการโจมตีที่อาจเกิดขึ้นด้วยการเปรียบเทียบค่าของไฟล์ที่น่าสงสัยกับตัวอย่างมัลแวร์ที่เคยถูกจัดหมวดหมู่ไว้ และจัดเก็บข้อมูลลำดับเหตุการณ์จากกระบวนการของโปรแกรมต่างๆ (Process ID) ของเครื่องคอมพิวเตอร์ลูกข่ายทั้งหมดตั้งแต่เริ่มต้นจนถึงสิ้นสุด เพื่อใช้ช่วยในการสืบสวนในเหตุการณ์ที่น่าสงสัยที่มีประสิทธิภาพและตอบสนองต่อเหตุการณ์ด้านความปลอดภัยด้านเทคโนโลยีสารสนเทศ ทั้งยังเพิ่มขีดความสามารถด้านการตรวจติดตามภัยคุกคามและความสามารถในการปฏิบัติการด้านความปลอดภัยด้านเทคโนโลยีสารสนเทศ

จึงจำเป็นต้องจัดหาระบบตรวจสอบและวิเคราะห์ภัยคุกคามเครื่องคอมพิวเตอร์ลูกข่าย (Endpoint Detection and Respond) เพื่อให้เห็นภาพรวมภัยคุกคามอย่างเต็มรูปและสามารถตรวจสอบและวิเคราะห์สาเหตุที่แท้จริงของการโจมตีหรือเหตุการณ์ต่างๆได้ พร้อมตอบสนองภัยคุกคามด้านเทคโนโลยีสารสนเทศที่มาจากเครื่องลูกข่ายได้ทันที

๒. วัตถุประสงค์

จัดหาระบบตรวจสอบและวิเคราะห์ภัยคุกคามเครื่องคอมพิวเตอร์ลูกข่าย (Endpoint Detection and Respond)

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 บุคคลหรือนิติบุคคลที่จะเข้าเป็นคู่สัญญาต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่ายหรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ

๓.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ สำนักงาน กสทช. ณ วันยื่นข้อเสนอ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม

๓.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ให้เช่าได้มีคำสั่งให้สละสิทธิ์ความคุ้มกันเช่นว่านั้น

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

๓.๑๑ ผู้ยื่นข้อเสนอราคาต้องได้รับแต่งตั้งให้เป็นตัวแทนจำหน่ายหรือเป็นผู้ให้เช่าระบบตรวจจับและป้องกันการบุกรุกเครือข่าย จากผู้ผลิต หรือสาขาของบริษัทผู้ผลิตประจำประเทศไทยและรับรองว่ามีความสามารถในการให้บริการติดตั้ง ซ่อมแซมแก้ไข ระบบตรวจจับและป้องกันการบุกรุกเครือข่ายและต้องมีหนังสือรับรองทางเทคนิคและการบำรุงรักษาตลอดระยะเวลาของสัญญา

๔. คุณลักษณะเฉพาะ

ระบบตรวจสอบและวิเคราะห์ภัยคุกคามเครื่องคอมพิวเตอร์แบบ Endpoint Detection and Respond (EDR) จำนวน ๑ ระบบ มีคุณสมบัติและคุณลักษณะเฉพาะอย่างน้อยดังนี้

๔.๑ มีความสามารถในการเฝ้าสังเกต (monitor), เก็บบันทึก (record), การสอบสวน (investigation) ด้านความปลอดภัยในปัจจุบันและย้อนหลังจากเครื่องลูกข่าย (endpoint) ได้

๔.๒ รองรับการบริหารจัดการเครื่องคอมพิวเตอร์ ได้ไม่น้อยกว่า ๒,๒๐๐ เครื่อง และรองรับการเพิ่มขยายได้ในอนาคต

๔.๓ สามารถเก็บรวบรวมข้อมูล metadata จาก Windows endpoint สำหรับการทำ investigation เพื่อหา affected endpoints ได้ โดยเก็บข้อมูลต่อไปนี้ได้เป็นอย่างน้อย

(๑) Host (name / IP address)

(๒) User account

(๓) File name

(๔) File path

(๕) Hash values (SHA-๑, SHA-๒๕๖ และ MD๕)

(๖) Registry key

(๗) Registry data

(๘) Registry name

(๙) Command line

๔.๔ จะต้องวิเคราะห์ผลกระทบของไฟล์ที่ต้องสงสัย (suspicious files), IP addresses และ domain ได้

๔.๕ สามารถทำ Preliminary Investigation เพื่อประเมินความเสี่ยง (assessment) ได้จากเกณฑ์ดังต่อไปนี้ได้เป็นอย่างน้อย

(๑) Host (Endpoint name, FQDN, IP address)

(๒) User account

(๓) File name

(๔) File path

(๕) Hash value

(๖) Registry key, Registry name และ Registry data

(๗) Command line

(๘) OpenIOC

๔.๖ สามารถทำ detailed investigation หรือ Live Investigations เพื่อตรวจสอบทุกไฟล์ที่อยู่บน disk ได้จาก OpenIOC rules และตรวจสอบทุก processes ที่กำลังทำงานอยู่ใน memory ได้จาก YARA rules

๔.๗ สามารถวิเคราะห์หาผลกระทบ (impact analysis) บนเครื่องที่ได้รับผลกระทบได้

๔.๘ สามารถทำ investigation ในการหา root cause analysis เพื่อแสดง objects ที่เกี่ยวข้องในเหตุการณ์ที่เกิดขึ้นในลักษณะ Analysis chain ได้จากเกณฑ์ดังต่อไปนี้

(๑) DNS record

(๒) IP address

(๓) File name

(๔) File path

(๕) SHA๑- hash values

(๖) MD๕ hash values

(๗) User account

๔.๙ มีตัวเลือกเพิ่มเติม หรือสามารถกำหนด action ได้ดังต่อไปนี้เป็นอย่างน้อย

(๑) Terminate Object เพื่อยุติการทำงาน object บน endpoint ที่เป็นเครื่องเป้าหมาย

(๒) Add to Suspicious Objects List เพื่อยุติการทำงานของ object บน endpoint ที่เป็นเครื่องเป้าหมาย และเพิ่ม object ได้แก่ File, IP address และ DNS (Domain และ URL) ไปยัง User-Defined Suspicious Object เพื่อป้องกันการแพร่กระจายของภัยคุกคามไปยังเครื่องลูกข่ายอื่น

(๓) Add to Preliminary Investigation List เพื่อนำ object ดังกล่าวมาเริ่มต้นทำการ investigation ใหม่

(๔) Isolate Endpoints เพื่อตัดการเชื่อมต่อ endpoints ออกจากเครือข่าย

๔.๑๐ ระบบที่นำเสนอจะต้องสามารถทำงานร่วมกับ Endpoint และ APT ที่ทางสำนักงาน กสทช. ใช้งานอยู่ซึ่งเป็นยี่ห้อ Trend Micro Apex One Endpoint และ Trend Micro Deep Discovery Analyzer (DDAN) ได้อย่างมีประสิทธิภาพ

๕. ระยะเวลาในการดำเนินการ

ภายใน ๙๐ วัน นับจากลงนามในสัญญา

๖. สิ่งที่ต้องส่งมอบ

ผู้ขายจะต้องส่งมอบงานทั้งหมดพร้อมทั้งอบรมการใช้งานระบบให้กับเจ้าหน้าที่ของสำนักงาน กสทช. อย่างน้อย ๕ คน ภายในระยะเวลาที่กำหนดในสัญญา

๗. วงเงินในการจัดหา

ภายในวงเงินงบประมาณ ๒,๐๘๙,๐๐๐.- บาท (สองล้านแปดหมื่นเก้าพันบาทถ้วน) โดยเบิกจ่ายจากงบประมาณรายจ่าย ประจำปี ๒๕๖๔ ของสำนักเทคโนโลยีสารสนเทศ (นบ.) หมวดค่าครุภัณฑ์ ที่ดิน และสิ่งก่อสร้าง รายการครุภัณฑ์คอมพิวเตอร์

๘. เกณฑ์การพิจารณาการคัดเลือกข้อเสนอ

สำนักงาน กสทช. จะพิจารณาคัดเลือกข้อเสนอโดยใช้เกณฑ์ราคา

๙. เงื่อนไขการชำระเงิน

สำนักงาน กสทช.จะชำระเงินเมื่อผู้ขายได้ส่งมอบระบบตรวจสอบและวิเคราะห์ภัยคุกคามเครื่องคอมพิวเตอร์ลูกข่าย (Endpoint Detection and Respond) ให้กับสำนักงาน กสทช. โดยจะต้องได้รับความเห็นชอบจากสำนักงาน กสทช. ว่าการดำเนินการเป็นไปอย่างครบถ้วน

๑๐. เงื่อนไขอื่นๆ

๑๐.๑ ผู้ขายจะต้องบำรุงรักษาและรับประกันการใช้งานระบบที่นำเสนอ ตลอดจนจะต้องรับผิดชอบดูแลแก้ไขปัญหาต่างๆ ที่เกิดขึ้นในระบบ รวมทั้งปรับแต่งระบบให้สามารถใช้งานได้อย่างมีประสิทธิภาพ เป็นระยะเวลา ๑ ปี

๑๐.๒ ผู้ขายตกลงบำรุงรักษาและซ่อมแซมแก้ไขระบบตรวจสอบและวิเคราะห์ภัยคุกคามเครื่องคอมพิวเตอร์ลูกข่าย (Endpoint Detection and Respond) ตามสัญญานี้ให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอ โดยให้มีเวลาขัดข้องรวมตามเกณฑ์การคำนวณเวลาขัดข้อง ไม่เกินเดือนละ ๓๖ ชั่วโมง หรือร้อยละ ๕ ของเวลาใช้งานทั้งหมดของเดือนนั้น (ชั่วโมงทำงานโดยนับ ๒๔ ชั่วโมงต่อ ๑ วันทำการ) แล้วแต่ตัวเลขใดจะมากกว่ากัน มิฉะนั้นผู้ขายต้องยอมให้ผู้ซื้อ คิดค่าปรับเป็นรายชั่วโมงในอัตราชั่วโมงละ ๐.๑% ของมูลค่าตามสัญญา ในช่วงเวลาที่ไม่สามารถใช้ได้ในส่วนที่เกินกว่ากำหนดเวลาขัดข้องข้างต้น

๑๑. อัตราค่าปรับ

ผู้ขายจะต้องติดตั้งและส่งมอบมอบงานแล้วเสร็จตามสัญญา มิฉะนั้นต้องชำระค่าปรับให้ สำนักงาน กสทช. เป็นรายวันในอัตราร้อยละ ๐.๒ (๐.๒%) ของมูลค่าของที่ยังไม่ได้ส่งมอบ จนถึงวันที่ผู้ขายได้ส่งมอบงาน ให้สำนักงาน กสทช. เป็นที่เรียบร้อยแล้ว ในระหว่างที่สำนักงาน กสทช. ยังไม่ได้ใช้สิทธิ์บอกเลิกสัญญานั้น หากสำนักงาน กสทช. เห็นว่าผู้ขายไม่อาจปฏิบัติตามสัญญาต่อไปได้ สำนักงาน กสทช. จะใช้สิทธิ์บอกเลิกสัญญากับเรียกร้องให้ชดใช้ราคาที่เพิ่มขึ้นจากราคาที่กำหนดไว้ในสัญญาถ้าสำนักงาน กสทช. ดำเนินการโดยซื้อจากบุคคลอื่นเต็มจำนวน หรือเฉพาะจำนวนที่ขาดส่ง และถ้าสำนักงาน กสทช. ได้แจ้งข้อเรียกร้องให้ชำระค่าปรับไปยังผู้ขายเมื่อครบกำหนดส่งมอบแล้ว สำนักงาน กสทช. มีสิทธิ์ที่จะปรับผู้ขายจนถึงวันบอกเลิกสัญญาได้อีกด้วย