รายละเอียดขอบเขตงานจ้างบริหารจัดการเฝ้าระวังภัยคุกคามของ สสวท. (CSOC)

1. ความเป็นมา

ตามที่ สสวท. มีนโยบายในการปรับรูปแบบการทำงานเป็น IPST Go Digital เพื่อให้สอดคล้องกับสถานการณ์และเทคโนโลยีในปัจจุบัน โดยมีการปรับปรุงกระบวนการทำงานให้สามารถปฏิบัติงานผ่านบริการระบบงานดิจิทัลและนวัตกรรม โดยจะมีข้อมูลสำคัญต่างๆ ที่ต้องจัดเก็บในระบบบริหารจัดการข้อมูลและระบบสนับสนุนสารสนเทศ ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2559 ในช่วงเวลาที่ผ่านมาได้มีกฎหมายและข้อบังคับที่ประกาศบังคับออกมาเพิ่มเติม ได้แก่ 1) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, 2) พระราชบัญญัติคอมพิวเตอร์ พ.ศ.2550 และ 3) ประกาศอื่น ๆ ที่เกี่ยวข้อง ซึ่ง ฝ่ายเทคโนโลยีสารสนเทศ ได้ดำเนินการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานแล้ว

จึงมีความจำเป็นในการใช้บริการเฝ้าระวังภัยคุกคามทางไซเบอร์ หรือ Cyber Security Operations Center (CSOC) เพื่อทำหน้าที่เฝ้าระวังและการบริหารความเสี่ยงในการรับมือภัยคุมคามทางไซเบอร์ ที่อาจเกิดขึ้นตลอดจนรองรับการปฏิบัติตามกฎหมายและข้อกำหนด (Compliance) นอกจากนี้ CSOC ยังช่วยสนับสนุนการบริหารจัดการเหตุการณ์ (Incident Management) และการพิสูจน์หลักฐานดิจิทัล (Forensics) เพื่อบรรเทา และลดความเสียหายต่อข้อมูลสำคัญและชื่อเสียงขององค์กร

2. วัตถุประสงค์

2.1 เพื่อยกระดับความพร้อมของหน่วยงานในการเฝ้าระวัง วิเคราะห์ และตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ สอดคล้องกับ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และ9 ตามแนวปฏิบัติของ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

2.2 เพื่อส่งเสริมให้การบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของหน่วยงานเป็นไปตามมาตรฐานสากล ISO/IEC 27001 โดยมุ่งเน้นการพัฒนาโครงสร้างพื้นฐาน กระบวนการ และการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Incident Management) ให้สามารถนำไปสู่การจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ได้ในอนาคต

2.3 เพื่อให้สามารถตรวจจับ วิเคราะห์ และแจ้งเตือนภัยคุกคามหรือเหตุการณ์ผิดปกติที่อาจกระทบต่อระบบสารสนเทศและข้อมูลสำคัญของหน่วยงานได้อย่างทันท่วงที โดยมีการบูรณาการการเฝ้าระวังแบบศูนย์กลาง (Centralized Security Monitoring) ครอบคลุมทั้งระบบเครือข่าย เครื่องแม่ข่ายคอมพิวเตอร์ ระบบคลาวด์ และโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล พร้อมสนับสนุนกระบวนการตอบสนองและกู้คืนระบบ (Response & Recovery) ให้เป็นไปตามแนวทางของ NIST Cybersecurity Framework (CSF)

3. คุณสมบัติผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงาน ของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดาเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและ การบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพรับจ้างงานดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอ ณ วันประกาศจัดซื้อจัดจ้าง หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม ในการยื่นข้อเสนอและเสนอราคาครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของ ผู้ยื่นข้อเสนอได้มีคาสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

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

3.11 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ เป็นไปตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ด่วนที่สุด ที่ กค (กวจ) ที่ ๐๔๐๕.๒ /ว๑๒๔ ลงวันที่ ๑ มีนาคม ๒๕๖๖

3.12 ผู้ยื่นข้อเสนอต้องมีผลงานในการบริหารจัดการระบบป้องกันตรวจจับและภัยคุกคามทางไซเบอร์ หรือผลงานในการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ จำนวน 1 ผลงาน วงเงินไม่น้อยกว่า 600,000 บาท (หกแสนบาทถ้วน) ในระยะเวลาไม่เกิน 3 ปี นับถัดจากวันสิ้นสุดภาระผูกพันตามสัญญา จนถึงวันที่ยื่นข้อเสนอ และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐ หรือหน่วยงานเอกชนที่ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) เชื่อถือ โดยยื่นสำเนาหนังสือรับรองผลงานและสำเนาสัญญาหรือใบสั่งซื้อ ซึ่งเป็นงานเดียวกัน

4. ขอบเขตงาน

ให้บริการเฝ้าระวังภัยคุกคาม วิเคราะห์ความเกี่ยวโยงของเหตุการณ์ และภัยคุกคามด้านความปลอดภัยสารสนเทศ (IT Security Monitoring Services) จากข้อมูลจราจรทางคอมพิวเตอร์ (Log) ของอุปกรณ์ต่างๆ ของที่เกี่ยวข้องทุกวันตลอด 24 ชั่วโมง และดำเนินการแจ้งเตือนเมื่อเกิดเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตาม Service Level Agreement (SLA) ที่กำหนด รวมทั้ง ให้คำแนะนำด้านเทคนิคในการแก้ไขเหตุการณ์ภัยคุกคามดังกล่าว โดยมีขอบเขตของงานดังนี้

4.1. จัดหาให้มีบริการระบบ Security Information & Event Management: SIEM ที่นำมาให้บริการภายในศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Operations Center: CSOC) ทั้งนี้ระบบ SIEM ที่นำมาให้บริการต้องมีคุณสมบัติ ดังนี้

4.1.1. ระบบจัดเก็บรวบรวมและส่งต่อข้อมูลจราจรทางคอมพิวเตอร์ (Log Collector) อยู่ในรูปแบบ Virtual Appliance ที่ออกแบบมาสำหรับทำงานร่วมกับระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (SIEM) โดยติดตั้งและให้บริการ ณ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.)

4.1.2. ระบบที่เสนอมีการทำงานแบบ Scale Out Architecture โดยมีหน่วยบริหารจัดการ (Supervisor) และหน่วยรวบรวมข้อมูล (Collector) เป็นอย่างน้อย

4.1.3. โดยระบบที่นำเสนอจะต้องทำการวิเคราะห์ข้อมูลและมีการเก็บข้อมูลที่ศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ตั้งอยู่ในประเทศไทย อย่างน้อย 2 ศูนย์ข้อมูล มีระยะทางห่างกันอย่างน้อย 100 กิโลเมตร และศูนย์คอมพิวเตอร์ (Data Center) ทุกแห่ง ต้องมีระบบเครือข่ายสื่อสารหลัก ที่เชื่อมเป็นเครือข่ายเดียวกันด้วยเทคโนโลยีบริหารจัดการระบบเครือข่าย (Software Define Infrastructure: SDI) เพื่อรองรับแผนการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Planning: BCP)

4.1.4. ผู้ยื่นข้อเสนอจะต้องสามารถรับและจัดเก็บข้อมูล Log จากแหล่งข้อมูล (Log Sources) ทั้งระบบภายในและระบบคลาวด์ (เช่น GDCC, Azure, AWS, GCP) ได้อย่างน้อยในรูปแบบ Syslog (TCP/UDP), SNMP, JDBC, WMI และ NetFlow โดยต้องเก็บ Raw Log อย่างน้อย 90 วัน ด้วยวิธีที่ปลอดภัย (เช่น Encryption, Access Control) และสามารถส่งมอบข้อมูลให้ สสวท. ได้ตามที่ร้องขอ

4.1.5. ผู้ยื่นข้อเสนอต้องสามารถรับเหตุการณ์จากอุปกรณ์เครือข่ายได้ไม่น้อยกว่า 60 อุปกรณ์ ได้เป็นอย่างน้อย

4.1.6. ผู้ยื่นข้อเสนอจะต้องรับและวิเคราะห์ข้อมูลได้ไม่น้อยกว่า 15,000 เหตุการณ์ต่อวินาที (Events per Second) และรองรับการเพิ่มขยายได้ในอนาคต

4.1.7. ผู้ยื่นข้อเสนอจะต้องสามารถให้บริการได้อย่างต่อเนื่อง โดยโครงสร้างระบบที่ให้บริการนั้นจะต้องถูกติดตั้งในรูปแบบ High Availability หรือดีกว่า

4.1.8. ระบบที่นำเสนอต้องอยู่ในศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ได้รับการรับรองมาตรฐานอย่างน้อยดังต่อไปนี้

1) มาตรฐานความปลอดภัยบนมาตรฐาน Healthcare ISO 27799

2) มาตรฐานการบริหารการรักษาความความปลอดภัย ISO/IEC 27001

3) มาตรฐานสากลสำหรับการปกป้องข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ ISO/IEC27018

4) มาตรฐานความปลอดภัยสำหรับระบบคลาวด์ CSA-STAR Cloud Security Level 2 (CSA STAR Level 2)

5) มาตรฐานการจัดการบริการด้านไอที ISO/IEC 20000-1

6) มาตรฐานด้านระบบบริหารจัดการความต่อเนื่องทางธุรกิจ ISO 22301:2019

7) มาตรฐานสากลสำหรับการรักษาความปลอดภัยของระบบคลาวด์ ISO/IEC 27017

4.1.9. ระบบต้องมีฐานข้อมูล Threat Intelligence ภายใต้เครื่องหมายการค้าเดียวกันกับ SIEM สามารถตรวจสอบความเสี่ยงจาก IP, Domain, Hash ได้

4.1.10. สามารถพิสูจน์ตัวตน (Authentication) ผู้ใช้งานได้ โดยรองรับฐานข้อมูลผู้ใช้แบบ Local, Microsoft AD, OpenLDAP, RADIUS และ SAML ได้เป็นอย่างน้อย

4.1.11. สามารถจัดทำรายงานแบบ Customized ได้ และรองรับการทำรายงานที่เกี่ยวข้องกับมาตรฐาน ISO27001, PCI, SANS, NIST ได้เป็นอย่างน้อย

4.1.12. สามารถแสดงผลของเหตุการณ์ที่ถูกตรวจจับโดยแยกตามหมวดหมู่ของ MITRE ATT&CK ได้

4.1.13. สามารถปิดบังข้อมูลบางส่วน เช่น User, Email, IP Address ด้วยวิธี Data Masking หรือ Data Obfuscation เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคลได้

4.1.14. รองรับคุณสมบัติ UEBA เพื่อช่วยในการตรวจสอบพฤติกรรมของผู้ใช้ในระบบได้ เมื่อทำงานร่วมกับ UEBA agent ในอนาคต

4.1.15. สามารถตรวจจับเหตุการณ์ผิดปกติที่สอดคล้องกับสิ่งบ่งชี้ภัยคุกคาม (Indicator of Compromise: IoC) เทียบกับฐานข้อมูลของเจ้าของผลิตภัณฑ์ โดยประกอบด้วย Domain, IP, URL และ Hash ได้เป็นอย่างน้อย

4.1.16. ผู้ยื่นข้อเสนอจะต้องสามารถรับและประมวลผลข้อมูลจากทั้งระบบเครือข่ายภายในและระบบคลาวด์ (Cloud Infrastructure / Services) ผ่านช่องทางต่าง ๆ ได้แก่ Logs, Performance Metrics, SNMP Traps, Security Alerts และ Configuration Change Events เพื่อรองรับการวิเคราะห์และเฝ้าระวังในสองมิติ ได้แก่ ตรวจสอบสถานะและสมรรถนะของระบบเครือข่าย (NOC) และ การตรวจจับ วิเคราะห์ และแจ้งเตือนภัยคุกคามทางไซเบอร์แบบเรียลไทม์ (SOC)

4.1.17. ต้องสามารถส่งข้อมูลเป็น IOC (Indicator of Compromise) มายังส่วนกลางได้

4.1.18. ผู้ยื่นข้อเสนอต้องสามารถแจ้งเตือนเมื่อมีเหตุการณ์ตรงตามเงื่อนไข (Correlation Rules) ที่สร้างไว้ และ เหตุการณ์ผิดปกติของตัวอุปกรณ์ผ่าน Email ได้เป็นอย่างน้อย

4.1.19. จัดหาให้มีบริการศูนย์เฝ้าระวังและแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์ (Cyber Security Operation Center: CSOC) โดยมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ เพื่อทำการวิเคราะห์และแจ้งเตือนภัยคุกคามฯ ให้กับสำนักงาน โดยมีขอบเขตการดำเนินด้านเฝ้าระวัง ตรวจจับการคุกคามทางไซเบอร์ ดังนี้

1) ต้องมีระบบการจัดเก็บ Ticket management หากพบเหตุการณ์ความผิดปกติด้าน Cyber security

2) ต้องจัดให้มีทีมงานที่มีความรู้ความสามารถในด้านการวิเคราะห์ เฝ้าระวัง และแจ้งเตือนภัยคุกคามด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เพื่อให้คำปรึกษาด้านเทคนิคตลอดระยะเวลาอายุสัญญา

3) แจ้งเตือนเมื่อตรวจพบภัยคุกคามหรือการบุกรุกระบบเทคโนโลยีสารสนเทศที่มีระดับความรุนแรงสำคัญ (Critical) หรือระดับความรุนแรงสูง (High) ผ่านทางอีเมล หรือโทรศัพท์ ตลอด 24 ชั่วโมง

4) ต้องสามารถจัดทำรายงานตามความต้องการของมาตรฐานความปลอดภัยต่าง ๆ ดังนี้ PCI, SOX, ISO/IEC 27001 หรือ ISO/IEC 27002, FISMA, HIPAA ได้เป็นอย่างน้อย

5) ต้องสามารถเลือกช่วงเวลาของข้อมูลดิบ (Raw Data) ที่จะค้นหาได้ ทั้งของช่วงเวลาปัจจุบันและของช่วงเวลาย้อนหลัง โดยระบุช่วงเวลาเริ่มต้นและสิ้นสุด

6) ต้องสามารถทำการจัดเก็บข้อมูลในลักษณะแบบ Online และ Offline (Raw Log) ได้

7) ต้องสามารถให้บริการได้อย่างต่อเนื่อง โดยมีระดับของการให้บริการ (Service Level Agreement) ไม่ต่ำกว่า 99.90% ต่อเดือน

8) ต้องปฏิบัติตามเงื่อนไขระดับของบริการ Service Level Agreement (SLA) ดังนี้

ระดับความรุนแรง	คำอธิบาย	เวลาในการตอบสนอง (Response time)
Critical	ผลกระทบกับระบบสารสนเทศหลักทำให้การดำเนินธุรกิจหยุดชะงักและจะต้องแก้ไขอย่างเร่งด่วนที่สุด	ภายใน 15 นาที
High	ผลกระทบกับระบบสารสนเทศที่ทำให้ธุรกิจไม่สามารถดำเนินการได้อย่างมีประสิทธิภาพ และจำเป็นต้องแก้ไขอย่างเร่งด่วน	ภายใน 3 ชั่วโมง
Medium	ผลกระทบกับระบบสารสนเทศทีมีผลต่อการดำเนินธุรกิจ และจำเป็นต้องแก้ไขอย่างทันท่วงที	ภายใน 6 ชั่วโมง
Low	ผลกระทบกับระบบสารสนเทศที่มีผลต่อประสิทธิภาพการทำงานทั่วไป แต่ไม่มีผลกระทบต่อการดำเนินธุรกิจโดยรวม	ภายใน 24 ชั่วโมง

9) ดำเนินงานบริการรับมือ และตอบสนองต่อภัยคุกคามทางไซเบอร์ (Incident Response) รายงานวิเคราะห์ปัญหาที่เกิดจากภัยคุกคาม (Incident Report) ซึ่งจะต้องประกอบด้วย

- ระบุประเภทของภัยคุกคาม
- วัน/เวลาที่ตรวจสอบพบ
- ต้นทาง (Source IP Address) และ ปลางทาง (Destination IP Address)
- อุปกรณ์ที่ได้รับผลกระทบ และระดับความรุนแรง (Severity)
- รายละเอียดของเหตุการณ์ที่เกิดขึ้น
- คำแนะนำ และขั้นตอนในการแก้ไข (Action & Recommendation)

4.2. ผู้ยื่นข้อเสนอจะต้องจัดทำแผนการปฏิบัติงาน การจัดการและแจ้งเตือนภัยคุกคาม (Incident Handling) ตลอดระยะเวลาตามสัญญา

4.3. ผู้ยื่นข้อเสนอจะต้องจัดให้มีทีมงานที่มีความรู้ความสามารถในด้านการวิเคราะห์ เฝ้าระวังและแจ้งเตือนภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร (IT Security Monitoring) และทีมผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศอื่นๆ ที่เกี่ยวข้อง เพื่อให้คำปรึกษาด้านเทคนิค หากมีการตรวจพบหรือตามที่ร้องขอ ตลอดระยะเวลาสัญญา

4.4. ผู้ยื่นข้อเสนอจะต้องจัดให้มีทีมงานสนับสนุนด้านการค้นคว้าและติดตามข้อมูลข่าวสารเกี่ยวกับความปลอดภัยเทคโนโลยีสารสนเทศ (Security Research Team) เพื่ออัพเดทข้อมูลข่าวสาร หรือข่าวสารที่ทันสมัย และ/หรือภัยคุกคามร้ายแรงด้านความปลอดภัยสารสนเทศ อย่างสม่ำเสมอ ตลอดระยะเวลาสัญญา

4.5. ผู้ยื่นข้อเสนอต้องมีการกำหนด เงื่อนไขการตรวจจับเหตุการณ์และรูปแบบการโจมตี (Correlation Rules และ Use Cases) เพื่อช่วยให้สามารถตรวจจับและแจ้งเตือนภัยคุกคามได้อย่างมีประสิทธิภาพและทันท่วงที โดยจะต้องจัดให้มี เงื่อนไขการตรวจจับ (Correlation Rules) จำนวนไม่น้อยกว่า 128 รายการ ครอบคลุมภัยคุกคามในกลุ่มต่าง ๆ และ ต้องสามารถเพิ่มเติม ปรับปรุง หรืออัปเดตเงื่อนไขการตรวจจับ (Correlation Rules / Use Cases) ได้อย่างต่อเนื่อง เพื่อให้สอดคล้องกับภัยคุกคามและข้อมูลจากระบบ Threat Intelligence ล่าสุด

4.6. ในกรณีเกิดเหตุการณ์ในระดับร้ายแรง และระดับวิกฤต ผู้ยื่นข้อเสนอจะต้องจัดทีม Computer Security Incident Response Team (CSIRT) พร้อมที่จะปฏิบัติหน้าที่ในการตอบสนองต่อเหตุการณ์และแก้ไขปัญหาที่เกิดขึ้น อย่างน้อย 1 ครั้ง หรือได้แจ้งผ่านทางโทรศัพท์ หรือ Email รวมถึงช่องทางการสื่อสารอื่นๆ ตามที่ สสวท. กำหนดได้ทุกวัน ไม่เว้นวันหยุด ภายใน 4 ชั่วโมง เพื่อวิเคราะห์หาสาเหตุของการบุกรุกและจัดลำดับความสำคัญของการบุกรุก พร้อมทั้งสนับสนุนข้อมูลที่มีการตรวจสอบด้านความมั่นคง

ปลอดภัยไซเบอร์ที่เกิดขึ้นร่วมกับหน่วยงานกลาง เช่น ThaiCERT, TB-CERT, หน่วยงานควบคุมและกำกับดูแลที่เกี่ยวข้องตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

4.7. ผู้ยื่นข้อเสนอจะต้องมีระบบบันทึกรายงานและแสดงสถานะการแก้ไขและรายงานผลการแก้ไขปัญหาเพื่อรายงานการเฝ้าระวังความปลอดภัยเทคโนโลยีสารสนเทศ (Security Monitoring) ในรูปแบบออนไลน์ และจัดประชุมเพื่อรายงานสรุปผลการจัดเก็บและการวิเคราะห์ข้อมูลประจำทุกเดือน โดยรายงานประจำเดือน ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

1) สรุปจำนวนเหตุการณ์ผิดปกติที่เกิดขึ้นทั้งหมด

2) สรุปจำนวนเหตุการณ์ที่เป็น Critical

3) สรุปจำนวนเหตุการณ์ทั้งหมดที่คุกคามระบบ โดยจำแนกตามสถานะความเร่งด่วน (Critical, High, Medium Low)

4) สรุปจำนวนเหตุการณ์ที่เกิดขึ้นในแต่ละวัน โดยจำแนกตามสถานะความเร่งด่วน (Critical, High, Medium Low)

5) สรุปเหตุการณ์ภัยคุกคามหรือเหตุการณ์ผิดปกติ (Incident or Event) ที่เป็นสาเหตุในการเกิดเหตุการณ์ผิดปกติ ที่เกิดขึ้นมากที่สุด 10 อันดับแรก

6) สรุปเหตุการณ์ที่เกิดขึ้นมากที่สุด 10 อันดับแรก จำแนกตามหัวข้อต่างๆ เช่น Rule Name, Source IP Address, Source Port, Target IP Address, Target Port เป็นต้น

7) สรุปรายการอุปกรณ์ ที่เฝ้าระวังภัยคุกคาม

8) สรุปจำนวน Ticket ที่เกิดขึ้นในรอบเดือน โดยจำแนกตามสถานะของ Ticket

9) สรุปรายละเอียดการทำงาน การวิเคราะห์เหตุการณ์ ของแต่ละ Ticket

10) สรุปการเรียกใช้ทีม CSIRT พร้อมรายงานที่เกี่ยวข้อง (ถ้ามี)

4.8. ต้องมีระบบแสดงสถานะการให้บริการและผลจากการวิเคราะห์เหตุการณ์ที่เกิดขึ้นในระบบออนไลน์ ได้โดยมีข้อมูลอย่างน้อยดังต่อไปนี้

1) สถานะของการเปิดและปิด Tickets

2) สถานะของ Incidents ที่เกิดขึ้น

3) สรุปผลการให้บริการ (Service History) และสถิติย้อนหลังได้ไม่น้อยกว่า 30 วัน

4.9. หาก สสวท. มีการทดสอบเจาะระบบสารสนเทศ ตามมาตรฐาน สากล (Vulnerability Scanning and Penetration Testing) ผู้ให้บริการต้องสนับสนุนข้อมูลส่วนของ Log และ รายงานการตรวจจับการโจมตีให้กับ สสวท. ทั้งนี้ สสวท. จะแจ้งก่อนการดำเนินการ ล่วงหน้าไม่น้อยกว่า 14 วัน

4.10. ผู้ยื่นข้อเสนอจะต้องมีการประเมินระดับความมั่นคงปลอดภัยทางไซเบอร์จากเครือข่ายภายนอก ตลอดระยะเวลาสัญญา โดยจะต้องนำข้อมูลจาก Threat Intelligence ที่อยู่ภายใต้เครื่องหมายการค้าเดียวกัน

เพื่อวิเคราะห์แสดงผลคะแนนเพื่อแสดงระดับความมั่นคงปลอดภัยทางไซเบอร์ โดยมีการอ้างอิง MITRE Cyber Threat Susceptibility Assessment (CTSA) และ Factor Analysis of Information Risk (FAIR) และ แสดงผลคะแนนจากระดับเทคนิค (Technical Rating)

4.11. ผู้ยื่นข้อเสนอจะต้องร่วมวิเคราะห์และปรับปรุง กระบวนการทำงานต่างๆ ที่เกี่ยวข้องกับโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ ระบบรักษาความปลอดภัยเทคโนโลยีสารสนเทศ ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของ สสวท. (เช่น นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ นโยบายการสำรองข้อมูลและการเตรียมความพร้อมในกรณีฉุกเฉินและอื่นๆ)

4.12. ผู้ยื่นข้อเสนอต้องจัดทำรายการวัสดุหรือครุภัณฑ์ที่ใช้ในงานจ้างซึ่งเป็นพัสดุที่ผลิตภายในประเทศ โดยต้องใช้ไม่น้อยกว่าร้อยละ 60 ของมูลค่าพัสดุที่จะใช้ในงานจ้างนี้ (ถ้ามี)

4.13. ปฏิบัติตามประกาศที่เกี่ยวข้องกับมาตรฐานต่างๆ ดังนี้

1) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

2) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

3) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566

4) ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566

5) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

5. บุคลากรในโครงการ

5.1 ผู้ยื่นข้อเสนอต้องมีบุคลากรที่มีความรู้ความเชี่ยวชาญในการปฏิบัติงานในศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามของผู้ให้บริการประจำในองค์กร ที่มีความเชี่ยวชาญในการเฝ้าระวังความปลอดภัยเทคโนโลยีสารสนเทศ พร้อมทั้งมีใบรับรอง (Certificate) ในด้านที่เกี่ยวข้อง ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องแนบสำเนาใบรับรอง ดังกล่าวมาพร้อมกับการยื่นข้อเสนอในครั้งนี้ โดยประกอบด้วยใบรับรอง ดังนี้

- การเจาะระบบอย่างมีจรรยาบรรณ EC-Council: Certified Ethical Hacker (CEH) อย่างน้อย 1 คน
- ความเชี่ยวชาญด้านการทดสอบการเจาะระบบ CompTIA: PenTest+ อย่างน้อย 1 คน

- ความรู้ด้าน Security ตามมาตรฐาน CompTIA: Security+ อย่างน้อย 1 คน

- ความเชี่ยวชาญด้าน Security ตามมาตรฐาน GIAC (GIAC Security Expert) หรือ ได้รับ Certified ISC2: Information Security Specialist Professional (CISSP) อย่างน้อย 1 คน

5.2 ผู้ยื่นข้อเสนอต้องมีเจ้าหน้าที่ในศูนย์ปฏิบัติการไม่น้อยกว่า 5 คน ประกอบไปด้วยบุคลากรดังนี้

- ผู้จัดการศูนย์ปฏิบัติการ SOC (SOC Manager) ในด้านการควบคุมการทำงานเฝ้าระวังและวิเคราะห์ภัยคุกคาม อย่างน้อย 1 คน

- เจ้าหน้าที่ผู้เชี่ยวชาญ (Security Analyst Tier 1) ในด้านการวิเคราะห์ภัยคุกคาม อย่างน้อย 1 คน

- เจ้าหน้าที่ผู้เชี่ยวชาญพิเศษ (Security Analyst Tier 2) ในด้านการบริหารจัดการระบบเฝ้าระวังและการวิเคราะห์ภัยคุกคามไซเบอร์ขั้นสูง อย่างน้อย 1 คน

- วิศวกรระบบ (System Engineer) ในด้านการดูแลระบบเฝ้าระวังฯ อย่างน้อย 2 คน

6. หลักเกณฑ์และสิทธิในการพิจารณาราคา

ในการพิจารณาผลการยื่นข้อเสนอครั้งนี้ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) จะพิจารณาตัดสิน โดยใช้หลักเกณฑ์ราคา เพียงอย่างเดียว และ การพิจารณาผู้ชนะการยื่นข้อเสนอ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) จะพิจารณาจาก ราคารวม (รวมภาษีมูลค่าเพิ่มแล้ว) ที่เสนอราคาต่ำสุด

7. ระยะเวลาดำเนินงาน 12 เดือน นับถัดจากวันลงนามในสัญญา

8. กำหนดส่งมอบงานและการจ่ายเงิน

งวดที่ 1 สสวท. จะจ่ายเงินร้อยละ 10 ของมูลค่าตามสัญญา เมื่อผู้รับจ้างส่งมอบงาน ดังนี้

- ส่งมอบแผนการทำงานตลอดระยะเวลาตามสัญญา ภายใน 7 วัน นับถัดจากวันลงนามในสัญญา

- รายงานการติดตั้งอุปกรณ์หรือระบบที่ใช้ในการเฝ้าระวัง และ รายงานการฝึกอบรมในรูปแบบการสอนงาน (on the job training) ภายใน 15 วัน นับถัดจากวันลงนามในสัญญา

- รายงานตามขอบเขตงาน ข้อ 4.7 ในรูปแบบไฟล์เอกสารอิเล็กทรอนิกส์ PDF ประจำเดือนที่ 1 และคณะกรรมการตรวจรับได้ตรวจรับเรียบร้อยแล้ว

- จัดทำรายการวัสดุหรือครุภัณฑ์ที่ใช้ในงานจ้างซึ่งเป็นพัสดุที่ผลิตภายในประเทศ โดยต้องใช้ไม่น้อยกว่าร้อยละ 60 ของมูลค่าพัสดุที่จะใช้ในงานจ้างนี้ (ถ้ามี) ภายใน 60 วัน นับถัดจากวันลงนามในสัญญา

งวดที่ 2 สสวท. จะจ่ายเงินร้อยละ 8 ของมูลค่าตามสัญญา เมื่อผู้รับจ้างส่งมอบงานตามขอบเขตงาน ข้อ 4.7 ในรูปแบบไฟล์เอกสารอิเล็กทรอนิกส์ PDF ประจำเดือนที่ 2 และคณะกรรมการตรวจรับได้ตรวจรับเรียบร้อยแล้ว

งวดที่ 3 สสวท. จะจ่ายเงินร้อยละ 8 ของมูลค่าตามสัญญา เมื่อผู้รับจ้างส่งมอบงานตามขอบเขตงาน ข้อ 4.7 ในรูปแบบไฟล์เอกสารอิเล็กทรอนิกส์ PDF ประจำเดือนที่ 3 และคณะกรรมการตรวจรับได้ตรวจรับเรียบร้อยแล้ว

งวดที่ 4 สสวท. จะจ่ายเงินร้อยละ 8 ของมูลค่าตามสัญญา เมื่อผู้รับจ้างส่งมอบงานตามขอบเขตงาน ข้อ 4.7 ในรูปแบบไฟล์เอกสารอิเล็กทรอนิกส์ PDF ประจำเดือนที่ 4 และคณะกรรมการตรวจรับได้ตรวจรับเรียบร้อยแล้ว

งวดที่ 5 สสวท. จะจ่ายเงินร้อยละ 8 ของมูลค่าตามสัญญา เมื่อผู้รับจ้างส่งมอบงานตามขอบเขตงาน ข้อ 4.7 ในรูปแบบไฟล์เอกสารอิเล็กทรอนิกส์ PDF ประจำเดือนที่ 5 และคณะกรรมการตรวจรับได้ตรวจรับเรียบร้อยแล้ว

งวดที่ 6 สสวท. จะจ่ายเงินร้อยละ 8 ของมูลค่าตามสัญญา เมื่อผู้รับจ้างส่งมอบงานตามขอบเขตงาน ข้อ 4.7 ในรูปแบบไฟล์เอกสารอิเล็กทรอนิกส์ PDF ประจำเดือนที่ 6 และคณะกรรมการตรวจรับได้ตรวจรับเรียบร้อยแล้ว

งวดที่ 7 สสวท. จะจ่ายเงินร้อยละ 8 ของมูลค่าตามสัญญา เมื่อผู้รับจ้างส่งมอบงานตามขอบเขตงาน ข้อ 4.7 ในรูปแบบไฟล์เอกสารอิเล็กทรอนิกส์ PDF ประจำเดือนที่ 7 และคณะกรรมการตรวจรับได้ตรวจรับเรียบร้อยแล้ว

งวดที่ 8 สสวท. จะจ่ายเงินร้อยละ 8 ของมูลค่าตามสัญญา เมื่อผู้รับจ้างส่งมอบงานตามขอบเขตงาน ข้อ 4.7 ในรูปแบบไฟล์เอกสารอิเล็กทรอนิกส์ PDF ประจำเดือนที่ 8 และคณะกรรมการตรวจรับได้ตรวจรับเรียบร้อยแล้ว

งวดที่ 9 สสวท. จะจ่ายเงินร้อยละ 8 ของมูลค่าตามสัญญา เมื่อผู้รับจ้างส่งมอบงานตามขอบเขตงาน ข้อ 4.7 ในรูปแบบไฟล์เอกสารอิเล็กทรอนิกส์ PDF ประจำเดือนที่ 9 และคณะกรรมการตรวจรับได้ตรวจรับเรียบร้อยแล้ว

งวดที่ 10 สสวท. จะจ่ายเงินร้อยละ 8 ของมูลค่าตามสัญญา เมื่อผู้รับจ้างส่งมอบงานตามขอบเขตงาน ข้อ 4.7 ในรูปแบบไฟล์เอกสารอิเล็กทรอนิกส์ PDF ประจำเดือนที่ 10 และคณะกรรมการตรวจรับได้ตรวจรับเรียบร้อยแล้ว

งวดที่ 11 สสวท. จะจ่ายเงินร้อยละ 8 ของมูลค่าตามสัญญา เมื่อผู้รับจ้างส่งมอบงานตามขอบเขตงาน ข้อ 4.7 ในรูปแบบไฟล์เอกสารอิเล็กทรอนิกส์ PDF ประจำเดือนที่ 11 และคณะกรรมการตรวจรับได้ตรวจรับเรียบร้อยแล้ว

งวดที่ 12 สสวท. จะจ่ายเงินร้อยละ 10 ของมูลค่าตามสัญญา เมื่อผู้รับจ้างส่งมอบงานตามขอบเขตงาน ข้อ 4.7 ในรูปแบบไฟล์เอกสารอิเล็กทรอนิกส์ PDF ประจำเดือนที่ 12 และคณะกรรมการตรวจรับได้ตรวจรับเรียบร้อยแล้ว

9. การรับประกันผลงานหลังสิ้นสุดสัญญา

ภายหลังการดำเนินงานครบตามระยะเวลาสัญญา 12 เดือน ผู้ให้บริการต้องรับประกันผลงานการให้บริการศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์ (CSOC) เป็นระยะเวลาไม่น้อยกว่า 30 วัน นับถัดจากวันสิ้นสุดสัญญา เพื่อให้สามารถตรวจสอบและแก้ไขปัญหาความบกพร่อง (Defect / Error) ที่อาจเกิดขึ้นจากระบบหรือการให้บริการในช่วงเวลาดังกล่าวได้ โดยผู้ให้บริการต้องดำเนินการแก้ไขให้แล้วเสร็จภายในระยะเวลาที่ สสวท. กำหนด โดยไม่คิดค่าใช้จ่ายเพิ่มเติม การรับประกันนี้ให้ครอบคลุมถึงการให้คำปรึกษาเชิงเทคนิค (Technical Advisory) และการสนับสนุนการตรวจสอบเหตุการณ์ร้ายแรง (Critical Incident) ที่ยังคงส่งผลต่อความมั่นคงปลอดภัยของระบบงานในขอบเขตเดิมของสัญญา

10. ค่าปรับ

10.1 กรณีที่ผู้ยื่นข้อเสนอไม่สามารถดำเนินการ ตามข้อกำหนด ต้องชำระค่าปรับรายวันในอัตราร้อยละ 0.1 ของราคาค่าจ้าง ตามสัญญา

10.2 กรณีอุปกรณ์ของผู้ยื่นข้อเสนอ ไม่สามารถใช้งานได้และต้องส่งซ่อมแซม ผู้ยื่นข้อเสนอต้องนำอุปกรณ์ที่มีคุณสมบัติเทียบเท่าหรือดีกว่า มาสำรองใช้งานภายใน 24 ชั่วโมง และดำเนินการติดตั้งให้อุปกรณ์ที่นำมาทดแทนสามารถทำงานได้เป็นปกติ กรณีที่ไม่สามารถดำเนินการแก้ไขซ่อมแซม ภายใน 24 ชั่วโมง หลังจากได้รับแจ้งเหตุผิดปกติ ต้องชำระค่าปรับรายชั่วโมงในอัตราร้อยละ 0.1 ของราคาค่าจ้าง ตามสัญญา นับถัดจากเวลาที่ครบตามกำหนดจนถึงดำเนินการแก้ไขซ่อมแซมแล้วเสร็จ

11. ความรับผิดของผู้รับจ้าง

ผู้รับจ้างจะต้องรับผิดต่ออุบัติเหตุ ความเสียหาย หรือภยันตรายใดๆ อันเกิดจากการปฏิบัติงานของผู้รับจ้างและจะต้องรับผิดต่อความเสียหายจากการกระทำของลูกจ้างหรือตัวแทนของผู้รับจ้างและจากการปฏิบัติงานของผู้รับจ้างช่วงด้วย (ถ้ามี)

ความเสียหายใดๆ อันเกิดแก่งานที่ผู้รับจ้างได้ทำขึ้น แม้จะเกิดขึ้นเพราะเหตุสุดวิสัยก็ตาม ผู้รับจ้างจะต้องรับผิดชอบโดยซ่อมแซมให้คืนดีหรือเปลี่ยนให้ใหม่โดยค่าใช้จ่ายของผู้รับจ้างเอง เว้นแต่ความเสียหายนั้นเกิดจากความผิดของผู้ว่าจ้าง ทั้งนี้ ความรับผิดของผู้รับจ้างดังกล่าวในข้อนี้จะสิ้นสุดลงเมื่อผู้ว่าจ้างได้รับมอบงานครั้งสุดท้าย ซึ่งหลังจากนั้น ผู้รับจ้างคงต้องรับผิดเพียงในกรณีชำรุดบกพร่องหรือความเสียหายดังกล่าวในข้อ 4 เท่านั้น

ผู้รับจ้างจะต้องรับผิดต่อบุคคลภายนอกในความเสียหายใดๆ อันเกิดจากการปฏิบัติงานของผู้รับจ้าง หรือลูกจ้าง หรือตัวแทนของผู้รับจ้าง รวมถึงผู้รับจ้างช่วง (ถ้ามี) ตามสัญญานี้ หากผู้ว่าจ้างถูกเรียกร้องหรือฟ้องร้องหรือต้องชดใช้ค่าเสียหายให้แก่บุคคลภายนอกไปแล้ว ผู้รับจ้างจะต้องดำเนินการใดๆ เพื่อให้มีการว่าต่างแก้ต่างให้แก่ผู้ว่าจ้างโดยค่าใช้จ่ายของผู้รับจ้างเอง รวมทั้งผู้รับจ้างจะต้องชดใช้ค่าเสียหายนั้นๆ ตลอดจนค่าใช้จ่ายใดๆ อันเกิดจากการถูกเรียกร้อง หรือถูกฟ้องร้องให้แก่ผู้ว่าจ้างทันที