ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจ้างผู้ให้บริการเช่าใช้บริการ** Security Operation Center (SOC)

2. หน่วยงานเจ้าของโครงการ ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ

3. วงเงินงบประมาณที่ได้รับจัดสรร **6,000,000.- บาท (หกล้านบาทถ้วน)**

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 10 มีนาคม 2565

   เป็นเงิน **5,999,595.57 บาท (ห้าล้านเก้าแสนเก้าหมื่นเก้าพันห้าร้อยเก้าสิบห้าบาทเจ็ดสิบห้าสตางค์)** ราคา/หน่วย

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

   5.1 บริษัท อี-ซี.โอ.พี. (ประเทศไทย) จำกัด

   5.2 บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด

   5.3 บริษัท ซีเคียวอินโฟ จำกัด

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายฉัตรชัย	อาศรมเงิน	ผู้ช่วยผู้บริหารฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ
6.2 นายยศ	ดาราทิพย์	ผู้ช่วยผู้บริหารส่วนบริหารงานมาตรฐานเทคโนโลยีสารสนเทศ / ฝ่าย ปส.
6.3 นายกิตติ์ธเนศ	วงศ์ประสิทธิ์	ผู้ช่วยผู้บริหารส่วนบริการและปฏิบัติการเทคโนโลยีสารสนเทศ / ฝ่าย ปส.

ผนวก 1
ขอบเขตการดำเนินงาน
การจ้างผู้ให้บริการเช่าใช้บริการ Security Operation Center (SOC)

ผู้ยื่นข้อเสนอต้องเสนอบริการ โดยมีขอบเขตการดำเนินงานดังนี้

1. ข้อกำหนดความต้องการทั่วไป

1.1 ผู้ยื่นข้อเสนอต้องเป็นผู้ให้บริการการบริหารจัดการระบบความปลอดภัยสารสนเทศ (Managed Security Service Provider: MSSP) หรือ ประกอบกิจการศูนย์เฝ้าระวังด้านความปลอดภัยสารสนเทศ หรือความปลอดภัยไซเบอร์แบบครบวงจร ที่มีศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Security Operations Center: SOC) ตั้งอยู่ในประเทศไทย

1.2 ศูนย์ปฏิบัติการ Security Operations Center (SOC) ของผู้ยื่นข้อเสนอ ต้องได้รับมาตรฐานสากล ISO/ICE 27001 และมีความพร้อมในการให้บริการเฝ้าระวังและแจ้งเตือนเหตุการณ์ภัยคุกคามให้แก่ธนาคารตลอด 7 วัน 24 ชั่วโมง (7 x 24)

1.3 ผลิตภัณฑ์ที่ให้บริการทั้งหมด ผู้ยื่นข้อเสนอต้องมีสิทธิความเป็นเจ้าของหรือสิทธิการใช้งานอย่างถูกต้อง เพื่อให้บริการกับธนาคาร

1.4 ต้องเสนออุปกรณ์, โปรแกรมต่างๆ ,บริการ และส่วนประกอบเพิ่มเติมที่จำเป็นต่อการให้บริการให้ครบถ้วน หากบริการใดที่ธนาคารไม่ได้กำหนดและมีความจำเป็นต้องนำมาใช้งานร่วมกันเพื่อให้สามารถใช้บริการได้อย่างมีประสิทธิภาพ ผู้ยื่นข้อเสนอจะต้องจัดหาและส่งมอบให้กับธนาคารได้อย่างครบถ้วน

ส่วนที่ 1 การเตรียมระบบ

2. ความต้องการด้านเทคนิค

2.1 ต้องจัดเตรียมระบบเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ ซึ่งสามารถจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร ระบบจะต้องประกอบด้วยการทำงานดังต่อไปนี้

- สามารถวิเคราะห์และหาความสัมพันธ์ของข้อมูล เพื่อหาเหตุการณ์ผิดปกติได้
- สามารถปรับแต่งรูปแบบความสัมพันธ์หรือเงื่อนไข (Custom Rule) ได้
- สามารถแจ้งเตือนให้ผู้ดูแลระบบทราบ เมื่อตรวจพบข้อมูลที่สอดคล้องกับเงื่อนไขที่ได้ตั้งไว้
- สามารถจัดทำรายงาน หรือสรุปรายงานประจำเดือนได้
- สามารถบริการจัดการผ่าน Web Interface หรือ GUI ได้เป็นอย่างน้อย
- สามารถกำหนดสิทธิ์การเข้าถึงระบบ ตามระดับสิทธิ์การเข้าถึงได้ (Role Base Access Control)

2.2 ระบบเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ จะต้องสามารถรองรับข้อมูลจราจรทางคอมพิวเตอร์ได้ 100 GB/Day และจะต้องรองรับการทำงานหรือการเฝ้าระวัง ตามอุปกรณ์ดังต่อไปนี้ เป็นอย่างน้อย

- Firewall : Checkpoint, Paloalto, Juniper

- OS : Windows Server, RedHat, AS400
- Database : Oracle, Microsoft Sql, My Sql
- Network : Cisco, F5
- IPS : Tippingpoint
- WAF : Imperva
- Antivirus : Trendmicro
- Secure Internet Gateway : Zscaler

2.3 ต้องมี Disaster Recovery Site (DR Site) ที่ทำหน้าที่เป็นศูนย์ปฏิบัติการสำรอง ในกรณีที่ศูนย์ปฏิบัติการหลักของผู้ยื่นข้อเสนอไม่สามารถให้บริการได้ หรือ ระบบการเฝ้าระวังของผู้ยื่นข้อเสนอไม่สามารถให้บริการได้

2.4 ต้องจัดหาระบบเครือข่ายเชื่อมโยงศูนย์เทคโนโลยีสารสนเทศของธนาคาร และศูนย์ปฏิบัติหลักและศูนย์ปฏิบัติการสำรองของผู้ยื่นข้อเสนอ จำนวนอย่างน้อย 2 วงจร เพื่อใช้เป็นช่องทางหลัก 1 ช่องทาง และช่องทางสำรอง 1 ช่องทาง ในการส่งข้อมูลจราจรทางคอมพิวเตอร์โดยเฉพาะ ซึ่งต้องมีความเร็วของการส่งข้อมูลเพียงพอกับปริมาณข้อมูลจราจรทางคอมพิวเตอร์ที่ธนาคารจะส่งไปยังศูนย์ปฏิบัติการของผู้ยื่นข้อเสนอ และต้องเข้ารหัสข้อมูลจราจรทางคอมพิวเตอร์ก่อนที่จะส่งไปยังศูนย์ปฏิบัติการ

2.5 ต้องดำเนินการติดตั้งซอฟต์แวร์ (Log Collector) โดยธนาคาร จะเป็นผู้จัดหาฮาร์ดแวร์ที่มีประสิทธิภาพและความจุเพียงพอสำหรับรองรับปริมาณข้อมูลจราจรทางคอมพิวเตอร์ตามคำแนะนำของผู้ยื่นข้อเสนอ ซึ่งซอฟต์แวร์ดังกล่าวจะต้องมีคุณสมบัติดังต่อไปนี้

- สามารถทำหน้าที่ รับข้อมูลจราจรจากเครื่องต้นทาง มายังอุปกรณ์ดังกล่าวได้
- สามารถทำหน้าที่ ในการคัดกรอง Log ก่อนทำการส่งให้ระบบด้านความมั่นคงปลอดภัยเพื่อวิเคราะห์ต่อได้ เช่น SIEM เป็นต้น
- สามารถทำหน้าที่ ในการเก็บข้อมูลจราจรคอมพิวเตอร์ ได้ที่บนอุปกรณ์ ในกรณีที่ เครือข่ายเชื่อมโยงไม่สามารถใช้งานได้ หรือ ข้อมูลจราจรไม่สามารถส่งไปที่ศูนย์ปฏิบัติการของผู้ยื่นข้อเสนอได้ เป็นเวลาอย่างน้อย 1 วัน นับจากเวลาที่ไม่สามารถส่งข้อมูลไปที่ศูนย์ปฏิบัติการของผู้ยื่นข้อเสนอได้
- สามารถทำหน้าที่ ในการแจ้งเตือนในกรณีที่ ข้อมูลจราจร ไม่ส่งมายังตัวอุปกรณ์ได้
- สามารถรองรับปริมาณข้อมูลจราจรทางคอมพิวเตอร์ได้อย่างน้อย 150 GB/Day
- สามารถติดตั้งบนระบบ Virtual Machine (VMware) ได้

2.6 ต้องดำเนินการติดตั้งซอฟต์แวร์ Syslog Server โดยทางธนาคาร จะเป็นผู้จัดหาฮาร์ดแวร์ ที่มีประสิทธิภาพและความจุเพียงพอสำหรับรองรับข้อมูลปริมาณข้อมูลจราจรคอมพิวเตอร์ตามคำแนะนำข้อผู้ยื่นข้อเสนอ ซึ่ง ซอฟต์แวร์ ดังกล่าวจะต้องมีคุณสมบัติดังต่อไปนี้

- สามารถจัดเก็บ Log File ในรูปแบบของ Syslog หรือ SNMP หรือ sFlow หรือ NetFlow หรือ OPSEC ได้เป็นอย่างน้อย
- สามารถจัดเก็บ Log File ได้อย่างน้อย 100 GB/Day เป็นเวลาอย่างน้อย 120 วัน
- สามารถค้นหาข้อมูลได้ โดยสามารถค้นหาข้อมูลได้ดังต่อไปนี้ เช่น Syslog, SNMP traps หรือ Windows event logs เป็นต้น
- สามารถสร้างรายงาน และจัดส่งผ่านช่องทางอีเมลโดยอัตโนมัติและสามารถออกรายงานในรูปแบบ PDF หรือ CSV หรือ HTML
- สามารถตั้งระยะเวลาในการเก็บข้อมูลหรือ สั่งลบข้อมูลได้

- สามารถทำหน้าที่ ในการทำ Hashing เพื่อตรวจสอบความถูกต้องของ Logs หากถูกแก้ไขเปลี่ยนแปลงได้ ตามมาตรฐาน MD5 หรือ SHA1 หรือ SHA-256
- สามารถทำหน้าที่ในการบีบอัดข้อมูลของ Log ได้
- สามารถติดตั้งบนระบบ Virtual Machine (VMware) ได้

2.7 จัดให้มีผู้เชี่ยวชาญเข้าทำกระบวนการเตรียมพร้อมและส่งผ่านข้อมูลจราจรทางคอมพิวเตอร์ เพื่อใช้ในการเฝ้าระวังฯ (On-boarding process) ดังนี้

2.7.1 ตรวจสอบความพร้อมใช้ของระบบและอุปกรณ์ต้นกำเนิดข้อมูลจราจรทางคอมพิวเตอร์ที่จะใช้ในการ เฝ้าระวังร่วมกับเจ้าหน้าที่ของธนาคาร และให้คำแนะนำในการตั้งค่าอุปกรณ์เพื่อให้สามารถส่งข้อมูลจราจรทางคอมพิวเตอร์ได้

2.7.2 ระบุแหล่งที่มาของข้อมูลจราจรทางคอมพิวเตอร์และจัดหมวดหมู่ของอุปกรณ์ต้นกำเนิด

2.7.3 ระบุและวิเคราะห์ความเสี่ยงรูปแบบการโจมตี และจัดระดับของผลกระทบต่อระบบของทางธนาคารฯ รวมทั้งกำหนดประเภทข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่ต้องใช้ในการวิเคราะห์ร่วมกับธนาคาร

2.7.4 วิเคราะห์และสร้างแบบจำลองของภัยคุกคาม เพื่อหาวิธีและเครื่องมือในการเฝ้าระวังที่เหมาะสม (Threat Model)

2.7.5 จัดทำ Monitoring Use case ให้สอดคล้องกับ Threat Model และตั้งค่าระบบที่ใช้เฝ้าระวังฯ (SIEM) ตามที่กำหนดไว้ใน Monitoring Use case

2.7.6 จัดทำ Dashboard และ Alert ให้สอดคล้องกับ Monitoring Use case เพื่อใช้ในการแจ้งเตือนและรายงานต่างๆ

2.7.7 จัดทำแผนการทำงานร่วมกันในกระบวนการ Incident Management รวมถึงแผนการดำเนินการตอบโต้ภัยคุกคามร่วมกันกับทางธนาคาร

2.8 ให้คำแนะนำและประเมินกระบวนการตอบสนองต่อเหตุการณ์ผิดปกติ (Incident Response) ในปัจจุบันของธนาคาร เพื่อปรับปรุงกระบวนการตอบสนองต่อเหตุการณ์ผิดปกติให้มีประสิทธิภาพดีขึ้น

2.9 ให้คำแนะนำในการออกแบบระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) เพื่อจัดเก็บข้อมูล ณ ศูนย์เทคโนโลยีของธนาคาร ให้สอดคล้องตามนโยบายหรือข้อบังคับที่ทางธนาคารต้องปฏิบัติตาม

ส่วนที่ 2 การให้บริการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ ระยะเวลาให้บริการ 12 เดือน

2.10 บริการจัดเก็บและสืบค้นข้อมูลจราจรคอมพิวเตอร์ (Log Management)

2.10.1 จัดเก็บข้อมูลจราจรคอมพิวเตอร์ เป็นระยะเวลา 120 วัน ณ. ศูนย์เฝ้าระวังฯของผู้ให้บริการ และทำการสืบค้นข้อมูลจราจรคอมพิวเตอร์ ตามที่ธนาคารร้องขอ โดยมี SLA ดังนี้

Log ที่ร้องขอ	การสืบค้นข้อมูล
น้อยกว่า 30 วัน	ภายใน 24 ชั่วโมง
30 - 120 วัน	ภายใน 7 วันทำการ

2.10.2 ดำเนินการแยกประเภทข้อมูลจราจรทางคอมพิวเตอร์ ในกรณีที่จำเป็นต้องส่งข้อมูลจราจรทางคอมพิวเตอร์บางส่วนไปยังศูนย์ปฏิบัติการของผู้ยื่นข้อเสนอ และบางส่วนที่ต้องเก็บไว้ที่ศูนย์เทคโนโลยีของธนาคาร

2.10.3 บริการตรวจสอบสถานะการส่งจราจรทางคอมพิวเตอร์ พร้อมแจ้งเตือนไปยังเจ้าหน้าที่ที่เกี่ยวข้องของผู้ใช้บริการผ่านทางระบบอีเมล์ หรือช่องทางตามที่ตกลงกัน ในกรณีที่ตรวจพบว่าอุปกรณ์ทั้งหมดของธนาคารไม่สามารถส่งข้อมูลมายังศูนย์ปฏิบัติการของผู้ยื่นข้อเสนอ ผู้ยื่นข้อเสนอจะต้องแก้ไขให้สามารถส่งข้อมูลจราจรทางคอมพิวเตอร์ได้ภายในระยะเวลา 1.5 ชั่วโมง (90 นาที)

2.11 ดำเนินการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์เหตุการณ์ และแจ้งเตือนภัยคุกคามทางไซเบอร์ ให้แก่ธนาคาร ณ ศูนย์ปฏิบัติการของผู้รับจ้าง โดยให้บริการแบบตลอดเวลา 24 ชั่วโมงของทุกวัน ไม่มีวันหยุด (7 x 24) ตลอดระยะเวลาของสัญญา หากบริการการเฝ้าระวังความมั่นคงปลอดภัยของผู้ยื่นข้อเสนอไม่สามารถทำงานได้ ผู้ยื่นข้อเสนอจะต้องแก้ไขให้บริการเฝ้าระวังความความมั่นคงปลอดภัยสามารถใช้บริการได้ภายในระยะเวลา 1.5 ชั่วโมง (90 นาที)

2.12 แจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัย สำหรับเหตุการณ์ที่อยู่ในขอบข่ายภัยคุกคามทางไซเบอร์ โดยจะต้องแจ้งเตือนผ่านทาง Email หรือทางโทรศัพท์ หรือช่องทางอื่นใด ตามที่จะตกลงร่วมกันกับธนาคาร ตาม Severity Level Agreement (SLA) อย่างน้อยดังต่อไป ดังนี้

ระดับความรุนแรง	แจ้งเตือนผู้รับบริการ	ให้คำแนะนำในการแก้ไข
วิกฤติ	ภายใน 0.5 ชั่วโมง (30 นาที)	ภายใน 1 ชั่วโมง (60 นาที)
สูง	ภายใน 1 ชั่วโมง (60 นาที)	ภายใน 2 ชั่วโมง (120 นาที)
กลาง	ภายใน 1.5 ชั่วโมง (90 นาที)	ภายใน 3 ชั่วโมง (180 นาที)
ต่ำ	ภายใน 2 ชั่วโมง (120 นาที)	ภายใน 4 ชั่วโมง (240 นาที)

2.13 การแจ้งเตือนจะต้องมีรายละเอียด อย่างน้อยดังนี้

- ระบุประเภทของภัยคุกคาม
- วัน-เวลา เริ่มต้นของภัยคุกคาม
- ระบุต้นทาง (Attacker) และปลายทาง (Target)
- ระบุระดับความรุนแรง (Severity)
- รายละเอียดเหตุการณ์และพฤติกรรมทั้งหมด
- ภาพการเชื่อมโยงเหตุการณ์ภัยคุกคามที่เกิดขึ้น
- คำแนะนำและขั้นตอนการดำเนินการแก้ไขด้านเทคนิค Action & Recommendation

2.14 ให้คำปรึกษาเกี่ยวกับบริการวิเคราะห์เฝ้าระวังภัยคุกคามต่างๆ ที่เกิดขึ้น และสนับสนุนการทำงานเกี่ยวกับการแก้ไข ป้องกันและรับมือกับภัยคุกคามได้ตลอด 24 ชั่วโมง

2.15 ดำเนินการวิเคราะห์แบบรวมศูนย์และจัดทำเงื่อนไขการโจมตี (Use case Management) เพื่อช่วยในการเฝ้าระวังและแจ้งเตือนภัยคุกคามด้วยรูปแบบและมาตรฐานของผู้รับจ้าง (Standard Usecase) รวมทั้งปรับปรุงและจัดทำการแจ้งเตือนภัยคุกคามด้วยรูปแบบเงื่อนไขเฉพาะ หรือเงื่อนไขอื่นๆ เพิ่มเติม (Custom Usecase) ให้เหมาะสมกับ ธนาคารฯ

2.16 สามารถตรวจจับเหตุการณ์การคุกคามครอบคลุมในเรื่องดังนี้ เป็นอย่างน้อย

1. Unauthorized Access
2. Malicious code
3. Inappropriate usage
4. Multiple component
5. Denial of service
6. Information Gathering
7. Malware
8. Suspicious Traffic
9. Vulnerability Scan
10. lateral movement

2.17 ให้บริการทีมงานสำหรับการรวบรวมข้อมูลภัยคุกคามทางไซเบอร์ที่มีการปรับปรุงให้ทันสมัยอยู่เสมอจากแหล่งต่างๆ จากทั่วทุกมุมโลก (Threat Intelligence) เพื่อการวิเคราะห์ข้อมูลภัยคุกคามร่วมกับระบบ SIEM หรือ SOC Technology เพิ่มเติม เพื่อทำให้ ธนาคารฯ สามารถรับมือกับภัยคุกคามไซเบอร์ได้ อย่างมีประสิทธิภาพมากยิ่งขึ้น

2.18 จัดให้มีบริการแจ้งข่าวสารซึ่งเกี่ยวข้องกับระบบรักษาความมั่นคงปลอดภัย ระบบคอมพิวเตอร์และระบบเครือข่ายที่เกิดขึ้น ผ่านทางอีเมล์ เช่น

- รายชื่อ และคุณลักษณะของมัลแวร์ (Malware)
- ช่องโหว่ใหม่ (Vulnerability) ของอุปกรณ์ในระบบเครือข่าย (Network Equipment)
- ช่องโหว่ใหม่ (Vulnerability) ของระบบปฏิบัติการ (Operating System)

- ช่องโหว่ใหม่ (Vulnerability) ของระบบฐานข้อมูลหลัก (Database)
- ช่องโหว่ใหม่ (Vulnerability) ของโปรแกรมต่างๆ ที่ผู้รับจ้างเห็นว่าจะก่อให้เกิดผล เสียหายต่อการดำเนินงานของ ธนาคารฯ

โดยข่าวสารดังกล่าวประกอบด้วยเนื้อหาที่สำคัญ เช่น คำอธิบายอย่างคร่าวๆ (Overview), คำอธิบายอย่างละเอียด (Description), ผลกระทบ (Impact), ระบบที่ได้รับผลกระทบ (System Affected), ทางแก้ไข (Solution) (ถ้ามี), อ้างอิง (Reference) เป็นต้น

2.19 จัดเตรียมหน่วยปฏิบัติการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์ (CSIRT) พร้อมที่จะปฏิบัติหน้าที่ในการตอบสนองต่อภัยคุกคามหรือการบุกรุกระบบอย่างทันท่วงที หรือเข้าดำเนินการสืบสวนและวิเคราะห์หาสาเหตุของปัญหา ภัยคุกคามที่เกิดขึ้น รวมถึงการตรวจพิสูจน์พยานหลักฐานทาง Digital เมื่อมีการร้องขอบริการจากทางธนาคารภายในระยะเวลา 4 ชั่วโมงนับตั้งแต่ที่ธนาคารร้องขอ ไม่เกินกว่า 12 เหตุการณ์ พร้อมจัดทำรายงานผลการดำเนินงานสรุปข้อมูลหลักฐานต่างๆ ที่ได้จากการตอบสนองต่อเหตุการณ์ภัยคุกคาม รวมถึงแนวทางในการป้องกันการเกิดซ้ำในอนาคต (Incident Response and Recommendations Report) ทันทีที่สามารถดำเนินการได้

2.20 จัดทำรายงานสรุปสถิติภัยคุกคามประจำเดือน (Monthly Report) ภายในรูปแบบที่กำหนดไว้จากทางผู้ให้บริการ โดยมีหัวข้อของรายงาน อย่างน้อยดังนี้

- สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report)
- สรุป 10 อันดับสูงสุดของการโจมตี
- สรุป 10 อันดับสูงสุดของเป้าหมายที่โดยโจมตี
- สรุป 10 อันดับสูงสุดของผู้เข้ามาโจมตี
- สรุป 10 อันดับสูงสุดของช่องทางที่ถูกใช้โจมตี
- สรุปปริมาณและสถานะการใช้งานข้อมูลจราจรทางคอมพิวเตอร์ประจำเดือนแยกตามอุปกรณ์
- บทวิเคราะห์แนวโน้มของภัยคุกคามต่างๆ ที่เกิดขึ้นในเดือนที่ผ่านมา
- บทวิเคราะห์ประเมินความเสี่ยงในเดือนที่ผ่านมา เพื่อพัฒนาแนวทางการเฝ้าระวังให้ครอบคลุมกับภัยคุกคามใหม่ (Use Cases Development)
- สรุปคำแนะนำ

2.21 บริการเข้าร่วมประชุมประจำเดือน ทั้งแบบประชุมทางไกล (Video Conference Monthly Meeting) หรือเข้าประชุม ณ. ที่ทำการธนาคารฯ สำนักงานใหญ่ (On-Site Monthly Meeting) โดยผู้ยื่นข้อเสนอจะต้องเข้าร่วมประชุมเพื่อสรุปผลงานบริการวิเคราะห์เฝ้าระวังภัยคุกคามต่างๆ ที่เกิดขึ้นกับ ธนาคาร ทุกๆ เดือน ตลอดสัญญาของการให้บริการ

2.22 ผู้ยื่นข้อเสนอต้องดำเนินการจัดการซ้อมแผนรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ในรูปแบบการฝึกซ้อมแผนบนโต๊ะ (Tabletop Exercise) จำนวนอย่างน้อย 2 แผน ต่อปี โดยมีเจ้าหน้าที่ที่เกี่ยวข้องของธนาคาร เข้าร่วมการฝึกซ้อมด้วย

3. บุคลากรในการดำเนินโครงการ

ผู้ยื่นข้อเสนอจะต้องมีผู้เชี่ยวชาญและเจ้าหน้าที่ที่ปฏิบัติงานในศูนย์เฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ (พนักงานประจำ ที่มีประสบการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ที่ได้รับการรับรองความรู้ความสามารถ และมีประกาศนียบัตรรับรองที่ยังไม่หมดอายุ จนถึงวันที่ยื่นข้อเสนอ ดังต่อไปนี้

3.1 CISSP (Certified Information System Security Professional) หรือ GIAC GCFA (GIAC Certified Forensic Analyst) หรือ GIAC GCIH (GIAC Certified Incident Handler) หรือ CISM (Certified Information Security Manager) หรือ CISA (Certified Information System Auditor) อย่างน้อย 1 คน

3.2 OSCP (Offensive Security Certified Professional) หรือ CEH (Certified Ethical Hacker) หรือ CHFI (Computer Hacking Forenic Investigator) อย่างน้อย 1 คน

3.3 CompTIA CySA+ หรือ CompTIA Security+ อย่างน้อย 4 คน

4. ด้านการฝึกอบรม

ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกต้องจัดฝึกอบรมเกี่ยวกับการใช้งานระบบ SOC จำนวน 1 รอบ รอบละไม่น้อยกว่า 2 คน พร้อมจัดทำเอกสารการฝึกอบรม ให้แก่เจ้าหน้าที่ธนาคาร โดยการอบรมในห้องอบรมหรืออบรมผ่านช่องทางออนไลน์ตามที่ธนาคารกำหนด