ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย

การจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ การจ้างผู้ให้บริการ Security Operation Center (SOC)

2. หน่วยงานเจ้าของโครงการ ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ

3. วงเงินงบประมาณที่ได้รับจัดสรร 4,500,000.00 บาท สี่ล้านห้าแสนบาทถ้วน

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ 24 ก.ค. 2569

   เป็นเงิน 3,205,250.00 บาท สามล้านสองแสนห้าพันสองร้อยห้าสิบบาทถ้วน

   ราคา/หน่วย (ถ้ามี)

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

   5.1 บริษัท ดาต้าฟาร์ม จำกัด

   5.2 บริษัท แบงคอก เอ็มเอสพี จำกัด

   5.3 บริษัท จีดีแอล กรุ๊ป จำกัด

   5.4 บริษัท ไคเบอร์ จำกัด

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายพงษ์เทพ	เลขะกุล	ผู้ช่วยผู้บริหารฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ
6.2 นางสาวศรัญญา	แวงวรรณ์	ผู้บริหารส่วนจัดซื้อเทคโนโลยีสารสนเทศ / ฝ่าย จธ
6.3 นายชานนท์	แท่นทองจันทร์	ผู้ช่วยผู้บริหาร ส่วนรักษาความปลอดภัยเทคโนโลยีสารสนเทศ / ฝ่าย ปส.

ผนวก 1

ขอบเขตการดำเนินงาน

การจ้างผู้ให้บริการ Security Operation Center (SOC)

ผู้ยื่นข้อเสนอต้องเสนอบริการ Security Operation Center (SOC) โดยมีขอบเขตการดำเนินงาน ดังนี้

1. **ข้อกำหนดความต้องการทั่วไป**

   1.1 ผู้ยื่นข้อเสนอต้องเป็นผู้ให้บริการการบริหารจัดการระบบความปลอดภัยสารสนเทศ (Managed Security Service Provider: MSSP) หรือ ประกอบกิจการศูนย์เฝ้าระวังด้านความปลอดภัยสารสนเทศหรือความปลอดภัยไซเบอร์แบบครบวงจร 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 ผู้ยื่นข้อเสนอต้องมีสิทธิความเป็นเจ้าของหรือสิทธิการใช้งานอย่างถูกต้องเพื่อให้บริการกับธนาคาร

   1.4 ต้องเสนออุปกรณ์, โปรแกรมต่างๆ, บริการ, การดำเนินการส่ง log จากอุปกรณ์หรือระบบงานของทางธนาคารไปประมวลผลที่ศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ และส่วนประกอบเพิ่มเติมที่จำเป็นต่อการให้บริการให้ครบถ้วน

2. **ความต้องการด้านเทคนิค**

   2.1 ต้องจัดเตรียมระบบเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ ซึ่งสามารถจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร ระบบจะต้องประกอบด้วยการทำงานดังต่อไปนี้

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

   2.2 ระบบเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ จะต้องสามารถรองรับข้อมูลจราจรทางคอมพิวเตอร์ได้เฉลี่ยรายเดือนไม่น้อยกว่า 80 GB/Day และจะต้องรองรับการทำงานหรือการเฝ้าระวัง ตามอุปกรณ์ดังต่อไปนี้ เป็นอย่างน้อย

   - Firewall : Checkpoint, Paloalto, Juniper, Fortinet, Cisco
   - OS : Windows Server, RedHat, AS400
   - Database : Oracle, Microsoft Sql, My Sql
   - Network : Cisco, F5 SSL VPN, F5-Load Balance, Radware, Huawei, Forescout
   - WAF : Cloudflare
   - Antivirus : Trendmicro
   - Secure Internet Gateway : Zscaler

- Cloud : INET, MS-Azure, AWS or Etc.

2.3 บริการจัดเก็บและสืบค้นข้อมูล (Log Management)

2.3.1 บริการจัดเก็บ Log เป็นระยะเวลา 365 วัน

2.3.2 บริการสืบค้น Log ที่อยู่ในระยะเวลา 90 วันได้ตามที่ธนาคารร้องขอ ภายใน 7 วัน

2.3.3 บริการตรวจสอบสถานการณ์ส่ง Log พร้อมแจ้งเตือนไปยังเจ้าหน้าที่ที่เกี่ยวข้องของผู้ใช้บริการผ่านทางระบบอีเมล์ หรือช่องทางตามที่ตกลงกัน ในกรณีที่ตรวจพบว่าอุปกรณ์ทั้งหมดของธนาคารไม่สามารถส่งข้อมูล Log มายังศูนย์ปฏิบัติการของผู้ยื่นข้อเสนอ ผู้ยื่นข้อเสนอจะต้องแก้ไขให้สามารถส่งข้อมูล Log ได้ภายในระยะเวลา 4 ชั่วโมง เริ่มนับจากเวลาที่อุปกรณ์ของ ธสน. สำหรับใช้ในการส่งข้อมูล Log ตามที่ได้ตกลงกับผู้เสนอราคาฯ ไม่สามารถดำเนินการได้

2.4 จัดให้มีผู้เชี่ยวชาญเข้าทำกระบวนการเตรียมพร้อมและส่งผ่านข้อมูลจราจรทางคอมพิวเตอร์ เพื่อใช้ในการเฝ้าระวังฯ (On-boarding process) ดังนี้

2.4.1 ตรวจสอบความพร้อมใช้ของระบบและอุปกรณ์ต้นกำเนิดข้อมูลจราจรทางคอมพิวเตอร์ที่จะใช้ในการ เฝ้าระวังร่วมกับเจ้าหน้าที่ของธนาคาร และให้คำแนะนำในการตั้งค่าอุปกรณ์เพื่อให้สามารถส่งข้อมูลจราจรทางคอมพิวเตอร์ได้

2.4.2 ระบุแหล่งที่มาของข้อมูลจราจรทางคอมพิวเตอร์และจัดหมวดหมู่ของอุปกรณ์ต้นกำเนิด

2.4.3 ระบุและวิเคราะห์ความเสี่ยงรูปแบบการโจมตี และจัดระดับของผลกระทบต่อระบบของทางธนาคาร รวมทั้งกำหนดประเภทข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่ต้องใช้ในการวิเคราะห์ร่วมกับธนาคาร

2.4.4 วิเคราะห์และสร้างแบบจำลองของภัยคุกคาม เพื่อหาวิธีและเครื่องมือในการเฝ้าระวังที่เหมาะสม (Threat Model)

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

2.4.6 จัดทำ Alert ให้สอดคล้องกับ Monitoring Use case เพื่อใช้ในการแจ้งเตือนและรายงานต่างๆ

2.4.7 จัดทำแผนการทำงานร่วมกันในกระบวนการ Incident Management รวมถึงแผนการดำเนินการตอบโต้ภัยคุกคามร่วมกันกับทางธนาคาร

2.5 ระบบที่นำเสนอจะต้องมีความสามารถด้านการบริหารจัดการเหตุการณ์และข้อมูลความมั่นคงปลอดภัยสารสนเทศ (Security Information and Event Management: SIEM) อย่างน้อย ดังนี้

2.5.1 ระบบสามารถทำการสรุปแบบ Multi-Stage Attack ได้ และสามารถปรับแต่งเรื่องของ Use Case ในแต่ละ Stage และช่วงเวลาที่เกิดต่างกันได้

2.5.2 ระบบสามารถทำ Lookup Table สามารถดึงข้อมูลโดยตรงจาก Relational Database ได้

2.5.3 ระบบสามารถทำ Data Masking ในระดับ Field Level ได้และรองรับการทำ Approval ได้

2.5.4 ระบบที่เสนอมี UEBA Profile แบบต้องมี Profile แยกตาม Functionality ของประเภทข้อมูล

2.5.5 ระบบที่เสนอต้องสามารถเชื่อมโยงเหตุการณ์หลายรายการที่กระจัดกระจาย (Incident Stitching) เป็นเหตุการณ์เดียวแบบอัตโนมัติ โดยอิงตามพฤติกรรมและความสัมพันธ์ของกิจกรรม

2.5.6 ระบบที่เสนอต้องมีระบบ Risk Scoring แบบไดนามิกโดยคะแนนความเสี่ยงปรับตามพฤติกรรมสะสมและเปรียบเทียบ Peer Group โดยอัตโนมัติ

2.5.7 ระบบที่เสนอต้องมี Use Case Library ที่ครอบคลุม MITRE ATT&CK Framework และสามารถใช้งานได้ทันทีโดยไม่ต้องพัฒนาใหม่ทั้งหมด โดยอนุญาตให้มีการปรับแต่ง ค่าพารามิเตอร์หรือ Threshold เพียงเล็กน้อย เพื่อให้สอดคล้องกับบริบทขององค์กร

2.5.8 ผลิตภัณฑ์ที่เสนอต้องได้รับการจัดอันดับในกลุ่ม Leader ของ Gartner Magic Quadrant for Security Information and Event Management (SIEM) ประจำปี 2025 และต้องได้รับการจัดอันดับในกลุ่ม Leader ติดต่อกันไม่น้อยกว่า 2 ปี

2.5.9 ต้องสามารถรับรองขีดความสามารถ Multi-Factor Authentication (MFA)

2.5.10 ผู้เสนอราคาต้องจัดให้มีกระบวนการวิเคราะห์และเชื่อมโยงเหตุการณ์แบบรวมศูนย์ (Centralized Correlation) พร้อมกำหนดเงื่อนไขการตรวจจับภัยคุกคาม (Use Case) โดยทีมผู้เชี่ยวชาญของผู้รับจ้าง เพื่อใช้ในการเฝ้าระวังและแจ้งเตือนภัยคุกคามตามมาตรฐาน และรูปแบบที่ผู้รับจ้างกำหนด โดย Use Case ที่จัดทำต้องอ้างอิงมาตรฐาน NIST Incident Categories หรือ MITRE ATT&CK Framework เป็นอย่างน้อย

2.5.11 สามารถรองรับการทำ UEBA ไม่ต่ำกว่า 1,000 License

2.6 ระบบที่นำเสนอจะต้องมีความสามารถด้าน Security Orchestration อย่างน้อยดังนี้

2.6.1 ระบบต้องมีเครื่องมือจัดการเวิร์กโฟลว์แบบรวมศูนย์ เพื่อประสานงานการดำเนินการระหว่างเครื่องมือและทีมความปลอดภัยต่าง ๆ

2.6.2 ระบบต้องมีการออกแบบ Playbook แบบภาพ (Visual) ผ่านการลากและวาง พร้อมรองรับเงื่อนไขแบบ Branching และ Looping

2.6.3 ระบบต้องมีจุดอนุมัติโดยมนุษย์ (Human-in-the-Loop) ภายในเวิร์กโฟลว์อัตโนมัติสำหรับการดำเนินการตอบสนองที่มีความเสี่ยงสูง

2.6.4 ระบบต้องมีการนำเข้า แยกวิเคราะห์ และกรองการแจ้งเตือนซ้ำซ้อนจากแหล่งที่รองรับทั้งหมดโดยอัตโนมัติ โดยไม่ต้องดำเนินการด้วยตนเอง

2.6.5 ระบบต้องมีการเสริมข้อมูลอุบัติการณ์โดยอัตโนมัติด้วยข่าวกรองภัยคุกคาม (เช่น ชื่อเสียง IP, การจับคู่ IOC, ข้อมูล CVE) ภายใน 60 วินาทีหลังรับแจ้งเตือน

2.6.6 ระบบต้องมีการจัดลำดับความสำคัญอุบัติการณ์โดยอัตโนมัติ อิงตามกฎการให้คะแนนความรุนแรง ความสำคัญของสินทรัพย์ และบริบทภัยคุกคามที่กำหนดค่าได้

2.6.7 ระบบต้องมีการรองรับงานอัตโนมัติแบบตามตาราง (Scheduled Tasks) ที่ทำงานได้โดยอิสระจากการแจ้งเตือนขาเข้า

2.6.8 ระบบต้องมีคอนเนกเตอร์สำเร็จรูปสำหรับ SIEM, EDR, Firewall, ระบบจัดการตัวตน และแพลตฟอร์มออกตั๋วผ่าน REST API หรือ Native SDK

2.6.9 ระบบต้องมีการรองรับการแลกเปลี่ยนข้อมูลสองทิศทางกับระบบภายนอกโดยใช้รูปแบบมาตรฐาน เช่น STIX/TAXII, CEF, JSON

2.6.10 ระบบต้องมีกรอบสร้างคอนเนกเตอร์แบบกำหนดเอง เพื่อให้ทีมสามารถสร้างการเชื่อมต่อกับเครื่องมือที่ยังไม่รองรับได้โดยไม่ต้องพึ่งพาผู้ขาย

2.7 ระบบต้องมี TIP (Threat Intelligence Platform) พร้อม Threat Intelligence Feeds ไม่น้อยกว่า 35 Feed

2.8 ระบบที่นำเสนอจะต้องมีความสามารถด้านการตอบสนองต่ออุบัติการณ์ความมั่นคงปลอดภัยไซเบอร์ (Incident Response: IR) อย่างน้อยดังนี้

2.8.1 ระบบต้องมีการดำเนินการกักกัน (Containment) โดยอัตโนมัติ เช่น การแยกโฮสต์ การปิดใช้บัญชี การบล็อกไฟร์วอลล์ เมื่อ Playbook ถูกทริกเกอร์

2.8.2 ระบบต้องมีการบันทึกลำดับเหตุการณ์ทั้งหมดของการตอบสนองต่ออุบัติการณ์แต่ละรายการแบบถาวร (Immutable) พร้อมระบุตัวตนผู้กระทำและเวลา

2.8.3 ระบบต้องมีการสร้างและจัดการเคสอุบัติการณ์โดยอัตโนมัติจากการแจ้งเตือนที่สัมพันธ์กัน โดยรวมเหตุการณ์ที่เกี่ยวข้องไว้ในบริบทการสืบสวนเดียวกัน

2.8.4 ระบบต้องมีการรองรับการทำงานร่วมกันของนักวิเคราะห์ภายในเคส ได้แก่ การบันทึกหมายเหตุ การมอบหมายงาน การแนบไฟล์ และความคิดเห็นแบบเธรด

2.8.5 ระบบต้องมีการติดตามการปฏิบัติตาม SLA ต่อเคส พร้อมการแจ้งเตือนการยกระดับที่กำหนดค่าได้เมื่อเกินเกณฑ์เวลาตอบสนอง

2.9 ให้คำแนะนำและประเมินกระบวนการตอบสนองต่อเหตุการณ์ผิดปกติ (Incident Response) ในปัจจุบันของธนาคาร เพื่อปรับปรุงกระบวนการตอบสนองต่อเหตุการณ์ผิดปกติให้มีประสิทธิภาพดีขึ้น

2.10 บริการ Commercial DarkWeb Digital Risk Protection ที่เป็น Commercial Tool จำนวน 1 บริการ โดยใช้ระบบที่เป็น Commercial แบบบริการระบบคลาวน์ (On Cloud) สำหรับ 1 งาน ที่มี 20 Keywords และ 30 Takedown เป็นอย่างน้อยที่คุณสมบัติของระบบสนับสนุนบริการต้องมีคุณสมบัติดังต่อไปนี้

2.10.1 มี Sub Module ของ Digital Risk Protection สำหรับ Data Leak Monitor ต่อไปนี้ได้เป็นอย่างน้อย

2.10.1.1 ระบบตรวจสอบความรั่วไหลของซอร์สโค้ด Code Repository ได้อย่างน้อยดังนี้ Github และ Git Lab

2.10.1.2 ระบบตรวจสอบความรั่วไหลของเอกสาร Documents and Open Buckets จากแหล่งอย่างน้อยดังนี้ Scribd, postman และ Pastebin

2.10.1.3 ระบบตรวจสอบความรั่วไหลของเครื่องคอมพิวเตอร์ Compromised Computers ได้โดยที่สามารถ Download ข้อมูลตัวอย่างจาก Stealer ได้จาก Info Stealer ดังต่อไปนี้ Redline, Raccoon, Stealc และ lummac2

2.10.1.4 ระบบตรวจสอบความรั่วไหลของ API Platform

2.10.1.5 ระบบตรวจสอบความรั่วไหลของหมายเลขบัตรเครดิต Credit Card Leaks โดยสามารถตรวจสอบ BIN (Bank Identification Number) ได้

2.10.2 มี Sub Module ของ Digital Risk Protection สำหรับ Phishing and Brand Monitor ต่อไปนี้ได้เป็นอย่างน้อย

2.10.2.1 ระบบตรวจสอบการปลอมแปลงของโดเมน Fake URLs and Phishing Domains โดยสามารถระบุ WHOIS Detail, Hosting Platform และสามารถระบุ Suspicious Domain และ URL ได้

2.10.2.2 ระบบตรวจสอบการปลอมแปลงของแอปพลิเคชันมือถือ Fake Mobile Apps สามารถตรวจสอบการฝาก Mobile Application บน 3rd Party Website เช่น fdroid ได้และทำการ Screenshot หน้าจอของ 3rd party Website อัติโนมัติ

2.10.2.3 ระบบตรวจสอบการพูดถึงบนแพลตฟอร์มโซเชียลมีเดีย Social Media Discussions

2.10.2.4 ระบบตรวจสอบการปลอมแปลงบนแพลตฟอร์มโซเชียลมีเดีย Fake Social Media Handles เพื่อตรวจสอบการการปลอมแปลง Brand ขององค์กรบน Facebook, Linkedin, Instagram ได้

2.10.2.5 ระบบตรวจสอบการปลอมแปลงบนแพลตฟอร์มโซเชียลมีเดีย Fake Call Centres เพื่อตรวจสอบ Call Centres ที่ไม่เกิดจากขององค์กรเองได้

2.10.3 มี Sub Module ของ Digital Risk Protection สำหรับ Dark Web Monitor Module ต่อไปนี้ได้เป็นอย่างน้อย

2.10.3.1 ระบบตรวจสอบการพูดถึงบนดาร์กเว็บ Dark Web Discussion เมื่อมีกลุ่ม Threat Actor พูดคุยเกี่ยวกับองกรณ์ในตลาดมืด โดย Capture ผลของหน้าตลาดมืดเช่น BlackhatWorld

2.10.3.2 ระบบตรวจสอบการพูดถึงบนระบบส่งข้อความทันที Messaging Platform จากช่องทาง Telegram และสามารถบันทึกบทสนทนาตัวอย่าง ณ เวลานั้นได้

2.10.3.3 ระบบตรวจสอบการพูดถึงบนระบบส่งข้อความทันที Credential Leaks โดยระบุรายละเอียด Username และ Password ที่หลุดไปในตลาดมืดพร้อมทั้งระบุถึงชื่อ combolist

2.10.3.4 ระบบตรวจสอบการพูดถึงบนระบบส่งข้อความทันที Malware Logs

2.10.4 มี Sub Module ของ Attack Surface Management สำหรับ Infrastructure Compliance Management ต่อไปนี้ได้เป็นอย่างน้อย

2.10.4.1 ระบบตรวจสอบ SSLScan เพื่อตรวจสอบ SSL Certificate ที่มีช่องโหว่, ใกล้หมดอายุ และ Weak Cipher Issue ได้

2.10.4.2 ระบบตรวจสอบ Network Scan ระบุ Port ที่ต้องการ Scan และระบุ Score ความเสี่ยงได้และแสดงสถานะการเปิด Port ย้อนหลังไปในอดีตได้

2.10.5 มี Sub Module ของ Cyber Threat Intelligence ต่อไปนี้ได้เป็นอย่างน้อย

2.10.5.1 มีระบบ Adversary Intel

2.10.5.2 มีระบบ Vulnerability Intel

2.10.5.3 มีระบบ Malware Intel

2.10.5.4 มี Threat Feed ที่เกี่ยวกับ Dark web, CVE, Ransomware และ Hacktivism ได้

2.10.5.5 มีฐานข้อมูล Threat Actor ไม่น้อยกว่า 20,000 records และสามารถระบุ Motivation, Region, First Seen and Last Activity ได้ และสามารถระบุ Targeted Countries/Industries ในแต่ละ Threat Actor ได้

2.10.6 แพลตฟอร์มจะต้องมีการ Certified ISO 27001:2022

2.10.7 สามารถระบุแหล่งต้นทางที่เผยแพร่ข้อมูลได้ เช่น User หรือ IP Address หรือ IP Geolocation

2.10.8 สามารถระบุแหล่งต้นทางของข้อมูลที่หลุดไปได้ เช่น Domain หรือ Subdomain หรือ IP Address

2.10.9 ต้องรวมบริการในการตรวจสอบ เฝ้าระวัง 24x7 และสนับสนุนการ การใช้งานตลอดอายุสัญญา

2.10.10 ระบบสามารถมี AI ช่วยในการทำ Threat Summary และสรุปรายละเอียดเคสเบื้องต้นเป็นรูปแบบ Timeline ได้

2.10.11 มีระบบ Incident Management ภายในตัว

2.10.12 มีระบบ Generate PDF Report ที่เป็น AI ที่ได้ Report PDF แบบสวยงามเกี่ยวกับ Event นั้น

3. การให้บริการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์

3.1 ให้บริการ Security Awareness โดยการจัดทำ Phishing Simulation อย่างน้อย 2 ครั้งต่อปี (ตามที่ธนาคารกำหนด)

3.2 ดำเนินการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์เหตุการณ์ และแจ้งเตือนภัยคุกคามทางไซเบอร์ให้แก่ธนาคาร ณ ศูนย์ปฏิบัติการของผู้รับจ้าง โดยให้บริการแบบตลอดเวลา 24 ชั่วโมงของทุกวัน ไม่มีวันหยุด (7 x 24) ตลอดระยะเวลาของสัญญา

3.3 แจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัย สำหรับเหตุการณ์ที่อยู่ในขอบข่ายภัยคุกคามทางไซเบอร์ โดยจะต้องแจ้งเตือนผ่านทาง Email หรือทางโทรศัพท์ หรือช่องทางอื่นใด ตามที่จะตกลงร่วมกันกับธนาคาร ตาม Severity Level Agreement (SLA) ดังต่อไปนี้

ระดับ ความรุนแรง	**ระยะเวลาแจ้งเตือนผู้รับบริการ** (นับจากเวลาที่ผู้เสนอราคาฯ ตรวจพบภัยคุกคามทางไซเบอร์)	**ระยะเวลาให้คำแนะนำในการแก้ไขปัญหาเสร็จสิ้น** (นับจากเวลาที่ผู้เสนอราคาฯ แจ้งแก่ ธสน.)
วิกฤติ ภัยคุกคามที่ส่งผลกระทบต่อระบบหรือข้อมูลที่สำคัญอย่างมาก ทำให้ระบบหยุดทำงาน หรือไม่สามารถใช้งานได้ และอาจก่อให้เกิดความเสียหายอย่างร้ายแรง	ภายใน 0.5 ชั่วโมง	ภายใน 1 ชั่วโมง
สูง ภัยคุกคามที่อาจส่งผลกระทบต่อระบบหรือข้อมูลที่สำคัญอย่างรุนแรง ทำให้ระบบไม่สามารถทำงานได้ตามปกติ	ภายใน 1 ชั่วโมง	ภายใน 2 ชั่วโมง

หรืออาจส่งผลกระทบต่อความปลอดภัยของข้อมูล		
กลาง ภัยคุกคามที่อาจส่งผลกระทบต่อระบบหรือข้อมูลบางส่วน แต่ไม่ถึงกับทำให้ระบบหยุดทำงาน หรือไม่สามารถใช้งานได้	ภายใน 1.5 ชั่วโมง	ภายใน 3 ชั่วโมง
ต่ำ ภัยคุกคามที่ไม่ส่งผลกระทบต่อระบบหรือข้อมูลที่สำคัญ หรืออาจส่งผลกระทบเพียงเล็กน้อย	ภายใน 2 ชั่วโมง	ภายใน 4 ชั่วโมง

3.4 การแจ้งเตือนจะต้องมีรายละเอียด อย่างน้อยดังนี้

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

3.5 ให้คำปรึกษาเกี่ยวกับบริการวิเคราะห์เฝ้าระวังภัยคุกคามต่างๆ ที่เกิดขึ้น และสนับสนุนการทำงานเกี่ยวกับการแก้ไข ป้องกันและรับมือกับภัยคุกคามได้ตลอด 24 ชั่วโมง

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

3.7 สามารถตรวจจับเหตุการณ์การคุกคามครอบคลุมในเรื่องดังนี้ เป็นอย่างน้อย

3.7.1 Unauthorized Access
3.7.2 Malicious code
3.7.3 Inappropriate usage
3.7.4 Denial of service
3.7.5 Information Gathering
3.7.6 Malware
3.7.7 Suspicious Traffic
3.7.8 Vulnerability Scan

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

3.9 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), อ้างอิง (Reference) เป็นต้น

3.10 จัดเตรียมหน่วยปฏิบัติการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์ (CSIRT) พร้อมที่จะปฏิบัติหน้าที่ในการตอบสนองต่อภัยคุกคามหรือการบุกรุกระบบอย่างทันท่วงที และเริ่มเข้าดำเนินการเพื่อสืบสวนและวิเคราะห์หาสาเหตุของปัญหา ภัยคุกคามที่เกิดขึ้น รวมถึงการตรวจพิสูจน์พยานหลักฐานทาง Digital ณ ที่เกิดเหตุ เมื่อมีการร้องขอบริการจากทางธนาคารภายในระยะเวลา 4 ชั่วโมงนับตั้งแต่ที่ธนาคารร้องขอ ไม่เกินกว่า 5 เหตุการณ์ พร้อมจัดทำรายงานผลการดำเนินงานสรุปข้อมูลหลักฐานต่างๆ ที่ได้จากการตอบสนองต่อเหตุการณ์ภัยคุกคาม รวมถึงแนวทางในการป้องกันการเกิดซ้ำในอนาคต (Incident Response and Recommendations Report) ทันทีที่สามารถดำเนินการได้

3.11 จัดทำรายงานสรุปสถิติภัยคุกคามประจำเดือน (Monthly Report) ภายในรูปแบบที่ธนาคารเห็นชอบและมีหัวข้อของรายงาน อย่างน้อยดังนี้

- รายงานสรุประดับความความรุนแรงของเหตุการณ์ที่ตรวจพบรายเดือน
- รายงานสรุประดับความเสี่ยงของเหตุการณ์ที่ตรวจพบรายเดือน
- รายงานสรุปจำนวนของเหตุการณ์ที่ตรวจพบจำแนกตาม Classification type
- รายงานสรุปสถานะของเหตุการณ์ที่ตรวจพบรายเดือน
- รายงานเหตุการณ์ที่ตรวจพบจำแนกตาม Classification type
- รายงานสรุปปริมาณการใช้งานข้อมูลจราจรทางคอมพิวเตอร์ประจำเดือน
- รายงานแสดงสถานะของ Log Source ที่ส่ง Log มา SIEM
- สรุปรายงาน และให้คำแนะนำเพิ่มเติม ในการป้องกันภัยคุกคาม

3.12 บริการเข้าร่วมประชุมประจำเดือน ทั้งแบบประชุมทางไกล (Video Conference Monthly Meeting) หรือเข้าประชุม ณ. ที่ทำการธนาคารฯ สำนักงานใหญ่ (On-Site Monthly Meeting) โดยผู้ยื่นข้อเสนอจะต้องเข้าร่วมประชุมเพื่อสรุปให้คำแนะนำและทุกๆ เดือน ตลอดสัญญาของการให้บริการ

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

4. บุคลากรในการดำเนินโครงการ

ผู้ยื่นข้อเสนอจะต้องมีผู้เชี่ยวชาญและเจ้าหน้าที่ที่ปฏิบัติงานในศูนย์เฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ พนักงานประจำที่มีประสบการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ที่ได้รับการรับรองความรู้ความสามารถและมีประกาศนียบัตรรับรอง (Certificate) ที่ยังไม่หมดอายุ จนถึงวันที่ยื่นข้อเสนอ ดังต่อไปนี้

4.1 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

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

4.3 CompTIA CySA+ หรือ CompTIA Security+ อย่างน้อย 4 คน