ขอบเขตของงาน

(Term of Reference : TOR)

โครงการจ้างบริการศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ และทดสอบความมั่นคงปลอดภัยของระบบสารสนเทศ กนอ. ประจำปี 2567

การนิคมอุตสาหกรรมแห่งประเทศไทย

Industrial Estate Authority of Thailand (IEAT)

มิถุนายน 2567

สารบัญ

ข้อกำหนดและขอบเขตงาน (Terms of Reference : TOR)
โครงการจ้างบริการศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์
และทดสอบความมั่นคงปลอดภัยของระบบสารสนเทศ กนอ. ประจำปี 2567

1. หลักการและเหตุผล

เนื่องจากปัจจุบัน มีภัยคุกคามทางไซเบอร์ที่เกิดขึ้นใหม่หลากหลายรูปแบบ เช่น Unknown Malware, Advanced Persistent Threat (APT) และ Ransomware ประเภทต่างๆ โดยในแต่ละวันจะมีการเกิดถูกโจมตีเป็นจำนวนมาก ซึ่งการนิคมอุสาหกรรมแห่งประเทศไทย (กนอ.) ได้ตระหนักถึงความสำคัญในการยกระดับการเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์และเพื่อให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยต้องมีมาตรการหรือการดำเนินการเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงขององค์กร หรือข้อมูลส่วนบุคคลที่ทางองค์กรมีการเก็บรวบรวมไว้ ซึ่งหนึ่งในการดำเนินการหลักที่ทางองค์กรพิจารณา คือ การบริการศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ เพื่อทำหน้าที่เฝ้าระวังและรับมือภัยคุกคามทาง ไซเบอร์ขององค์กรได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถช่วยให้องค์กรรับรู้ถึงสถานการณ์ภัยคุกคามทางไซเบอร์ ต่างๆ และระบุถึงเหตุการณ์ผิดปกติได้อย่างรวดเร็วและแม่นยำ รวมทั้งตอบสนองต่อเหตุการณ์ที่เกิดขึ้นได้ทันท่วงที

จากเหตุผลที่กล่าวข้างต้นทำให้ กนอ. มีความประสงค์จะดำเนินการจ้างบริการตรวจสอบช่องโหว่ (Vulnerability Assessment: VA) และทดสอบเจาะระบบ (Penetration Testing) และใช้บริการศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ (SOC) เพื่อทำหน้าที่เฝ้าระวังและการบริหารความเสี่ยงในการรับมือภัยคุกคามทางไซเบอร์ให้ครอบคลุม รวมทั้งความรู้ความสามารถของบุคลากร ให้สอดคล้องกับนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ ของ กนอ. และโครงสร้างระบบเทคโนโลยีที่เป็นส่วนประกอบของการรักษาความปลอดภัยทางไซเบอร์ ได้อย่างมีประสิทธิภาพ

2. วัตถุประสงค์

2.1 เพื่อจัดหาการบริการตรวจสอบและเฝ้าระวังภัยคุกคามไซเบอร์ พร้อมได้รับคำแนะนำสนับสนุนจากผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์

2.2 เพื่อยกระดับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ตามมาตรฐานสากล โดยการเฝ้าระวังและเตรียมความพร้อมรับมือกับภัยคุกคามด้านไซเบอร์ ตลอด 24 ชั่วโมง ซึ่งสอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2.3 เพื่อสร้างความตระหนักให้กับเจ้าหน้าที่ของ กนอ. ให้มีความพร้อมสำหรับการรับมือต่อภัยคุกคามทางไซเบอร์

3. คุณสมบัติผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 ผู้ยื่นข้อเสนอต้องเป็นนิติบุคคลผู้มีอาชีพรับจ้างงานดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ กนอ. ณ วันยื่นข้อเสนอ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการเสนอราคาครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่ รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

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

3.11 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันที่ยื่นข้อเสนอ

(2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า 2 ล้านบาท

(3) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน 500,000 บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคลธรรมดา โดยพิจารณาจากบัญชีเงินฝากธนาคาร ณ วันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่ง ในวันลงนามในสัญญา

(4) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน)

3.12 ผู้ยื่นข้อเสนอต้องได้รับรองมาตรฐาน ISO/IEC 27001:2013 สำหรับศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ (Security Operations Center: SOC ซึ่งตั้งอยู่ในประเทศไทย โดยมีเจ้าหน้าที่ประจำปฏิบัติงานในศูนย์ฯ ตลอด 24 ชั่วโมงต่อวัน 7 วันต่อสัปดาห์ (24/7) ทั้งนี้ เจ้าหน้าที่ประจำปฏิบัติงานในศูนย์ฯ จะต้องเป็นพนักงานประจำของผู้รับจ้าง และไม่ใช่การจ้างพนักงานแบบชั่วคราว (Outsource)

3.13 ผู้ยื่นข้อเสนอต้องมีศูนย์บริการเฝ้าระวังด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Operation Center : SOC) โดยให้บริการตลอด 24 ชั่วโมงต่อวัน 7 วันต่อสัปดาห์ (24x7) และให้บริการอยู่ในปัจจุบันอย่างน้อย 1 โครงการ มีระยะเวลาบริการตามสัญญาไม่น้อยกว่า 1 ปี ซึ่งเป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐ หรือหน่วยงานเอกชนที่ กนอ. เชื่อถือ ทั้งนี้ ผู้ยื่นข้อเสนอต้องแสดงหนังสือรับรองผลงานหรือสำเนาสัญญาฯ หรือเอกสารยืนยันการจ้างพร้อมกับการยื่นข้อเสนอด้วย

3.14 ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทยสำหรับระบบตรวจจับและตอบสนองต่อภัยคุกคามสำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (Endpoint Detection and Response : EDR) ตามขอบเขตงานข้อ 4.9 และระบบป้องกันการโจมตีทางเว็บไซต์ (Web Application Firewall) ตามขอบเขตงานข้อ 4.11 ว่าสามารถให้บริการระบบดังกล่าวได้โดยถูกต้องตามกฎหมาย

4. ขอบเขตการดำเนินงาน

ผู้รับจ้างต้องดำเนินการให้บริการศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์และทดสอบความมั่นคงปลอดภัยของระบบสารสนเทศ การนิคมอุตสาหกรรมแห่งประเทศไทย ประจำปี 2566 – 2567 โดยมีรายละเอียดการดำเนินงาน ดังต่อไปนี้

4.1 <u>จัดทำแผนการดำเนินงาน</u>

4.1.1 แผนประเมินความเสี่ยงทางดิจิทัลพร้อมจัดทำรายงาน และแผนความเสี่ยง/ผลกระทบที่อาจเกิดขึ้นจากการดำเนินการตรวจสอบช่องโหว่ (VA) และทดสอบเจาะระบบ (Penetration Testing)

4.1.2 กำหนดเป้าหมายของอุปกรณ์ที่จะตรวจสอบช่องโหว่ (VA) จำนวนไม่น้อยกว่า 80 IP Address

4.1.3 จัดทำแผนการดำเนินงานโดยระบุ วัน เวลา สถานที่และบุคลากรที่ดำเนินการตรวจสอบช่องโหว่และทดสอบเจาะระบบ โดยบุคลากรที่เป็นผู้รับผิดชอบจะต้องดำเนินการด้วยตนเองตลอดระยะเวลาตามแผนการดำเนินงาน

4.1.4 แผนผังของบุคลากรและช่องทางการติดต่อสื่อสารของผู้รับจ้าง

4.1.5 รายละเอียดของซอฟต์แวร์สำหรับการตรวจสอบช่องโหว่และทดสอบเจาะระบบ

4.1.6 แผนการติดตั้งอุปกรณ์จัดเก็บข้อมูล Log จากเครื่องแม่ข่ายหรืออุปกรณ์เครือข่าย เข้าสู่ระบบวิเคราะห์ข้อมูลระบบ SIEM ของผู้รับจ้าง

4.1.7 แผนการติดตั้งระบบตรวจจับและตอบสนองต่อภัยคุกคามสำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (Endpoint Detection and Response : EDR)

4.1.8 แผนการติดตั้งระบบป้องกันการโจมตีทางเว็บไซต์ (Web Application Firewall : WAF)

ทั้งนี้ ให้จัดทำและส่งมอบให้ กนอ. ภายใน 15 วัน นับถัดจากวันลงนามในสัญญา

4.2 ดำเนินการตรวจสอบช่องโหว่ (VA)

4.2.1 ตรวจสอบช่องโหว่ (VA) ครั้งที่ 1 ของอุปกรณ์เครือข่าย (Network Equipment) และเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของ กนอ. จำนวนไม่น้อยกว่า 80 IP Address โดยใช้โปรแกรมประเภทที่มีลิขสิทธิ์และผู้รับจ้างมีสิทธิ์ใช้โดยถูกต้องตามกฎหมาย 1 โปรแกรม และ Open Source หรือ Freeware 1 โปรแกรม

4.2.2 วิเคราะห์ และจัดลำดับความเสี่ยง และจัดทำข้อเสนอแนะแนวทางการปิดช่องโหว่ที่ตรวจพบ จากการตรวจสอบช่องโหว่ (VA) ครั้งที่ 1

4.2.3 ร่วมดำเนินการให้คำปรึกษากับผู้ดูแลระบบของ กนอ. เพื่อปิดช่องโหว่ตามผลการตรวจสอบช่องโหว่ (VA) ครั้งที่ 1 ซึ่งเป็นช่องโหว่ที่สามารถดำเนินการแก้ไขได้ และไม่กระทบกับระบบงานของ กนอ. ตามขอบเขตของงานและระยะเวลาการดำเนินการที่ กนอ. เห็นชอบ และจัดทำรายงานผลการปิดช่องโหว่ครั้งที่ 1 โดยนำเสนอต่อ กนอ. อย่างละเอียด

4.2.4 ตรวจสอบช่องโหว่ (VA) ครั้งที่ 2 ของอุปกรณ์เครือข่าย (Network Equipment) และเครื่องแม่ข่าย (Server) ของ กนอ. จำนวนไม่น้อยกว่า 80 IP Address ซึ่งมีรายการอุปกรณ์ไม่น้อยกว่าการตรวจสอบช่องโหว่ในครั้งที่ 1 โดยใช้โปรแกรมประเภทมีลิขสิทธิ์ 1 โปรแกรม และ Open Source หรือ Freeware 1 โปรแกรม

4.2.5 วิเคราะห์ จัดลำดับความเสี่ยง และให้คำปรึกษากับผู้ดูแลระบบของ กนอ. จัดทำข้อเสนอแนะแนวทางการปิดช่องโหว่ที่ตรวจพบ จากการตรวจสอบช่องโหว่ (VA) ครั้งที่ 2

4.2.6 ร่วมดำเนินการให้คำปรึกษากับผู้ดูแลระบบของ กนอ. เพื่อปิดช่องโหว่ตามผลการตรวจสอบช่องโหว่ (VA) ครั้งที่ 2 ซึ่งเป็นช่องโหว่ที่สามารถดำเนินการแก้ไขได้ และไม่กระทบกับระบบงานของ กนอ. ตามขอบเขตของงานและระยะเวลาการดำเนินการที่ กนอ. เห็นชอบ และจัดทำรายงานผลการปิดช่องโหว่ครั้งที่ 2 โดยนำเสนอต่อ กนอ. อย่างละเอียด

4.3 ดำเนินการทดสอบเจาะระบบ (Penetration Testing)

4.3.1 ทดสอบเจาะระบบฐานข้อมูลสนับสนุนการระงับเหตุ (DSS) ครั้งที่ 1 ในรูปแบบ Grey-Box จำนวน 2 Roles

4.3.2 วิเคราะห์ และจัดลำดับความเสี่ยง โดยอ้างอิงตาม OWASP Top 10 เวอร์ชั่นล่าสุด หรือมาตรฐาน สากลอื่นๆ ที่เกี่ยวข้อง และจัดทำข้อเสนอแนะแนวทางการปิดช่องโหว่ที่ตรวจพบ จากการทดสอบเจาะระบบฐานข้อมูลสนับสนุนการระงับเหตุ (DSS) (Penetration Testing) ครั้งที่ 1

4.3.3 ทดสอบเจาะระบบฐานข้อมูลสนับสนุนการระงับเหตุ (DSS) ครั้งที่ 2 ในรูปแบบ Grey-Box จำนวน 2 Roles

4.3.4 วิเคราะห์ และจัดลำดับความเสี่ยง โดยอ้างอิงตาม OWASP Top 10 เวอร์ชั่นล่าสุด หรือมาตรฐาน สากลอื่นๆ ที่เกี่ยวข้อง และจัดทำข้อเสนอแนะแนวทางการปิดช่องโหว่ที่ตรวจพบ จากการทดสอบเจาะระบบฐานข้อมูลสนับสนุนการระงับเหตุ (DSS) (Penetration Testing) ครั้งที่ 2

4.4 <u>บริการศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ (Security Operation Center : SOC)</u>

ผู้รับจ้างจะต้องมีบริการศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ตลอด 24 ชั่วโมงต่อวัน 7 วันต่อสัปดาห์ (24/7) เพื่อให้ กนอ. ได้รับการแจ้งเตือนภัยคุกคามทางไซเบอร์และวิธีการตรวจสอบและแก้ไขได้อย่างถูกต้องมีประสิทธิภาพ โดยมีรายละเอียดการดำเนินงานดังต่อไปนี้

4.4.1 ต้องจัดเตรียมระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ โดยระบบจะต้องมีคุณสมบัติและขีดความสามารถดังต่อไปนี้

(1) ต้องรองรับปริมาณ Log รวมกันต่อวันทั้งหมดไม่เกิน 75 GB ต่อวัน

(2) ต้องมีซอฟแวร์สำหรับการส่งต่อข้อมูล (Forwarder or Sensor Agent) จากคอมพิวเตอร์แม่ข่ายที่ใช้ระบบปฏิบัติการ Windows Server หรือ Linux ได้เป็นอย่างน้อย

(3) ต้องมีหน้าแสดงผล (Dashboard) สำหรับการวิเคราะห์ข้อมูลที่มีโอกาสเป็นภัยคุกคาม และมีความสามารถ ดังต่อไปนี้

- สามารถสร้าง Dashboard ใหม่ได้
- สามารถปรับแต่ง Dashboard ได้
- สามารถลบ Dashboard ได้
- สามารถคัดลอก(Clone) Dashboard ได้
- สามารถส่งออกเป็นไฟล์ PDF ได้
- สามารถส่งนำเข้าเป็น JSON หรือ CSV ไฟล์ได้

(4) ต้องมีการแสดงผลของ Alert เพื่อให้ครอบคลุมการตรวจจับภัยคุกคามหรือสิ่งผิดปกติ โดยอ้างอิงตาม Security Kill Chain และ Mitre Attack

(5) ต้องสามารถทำค้นหาภัยคุกคามทางไซเบอร์ ได้แบบอัตโนมัติ (Automated Threat Hunting) เพื่อตรวจสอบภัยคุกคามเชิงรุก

4.4.2 ต้องจัดให้มีระบบรวบรวมข้อมูลจราจรทางคอมพิวเตอร์ (Log File) จากเครื่องแม่ข่าย หรืออุปกรณ์เครือข่าย เข้าสู่ระบบวิเคราะห์ข้อมูลระบบ SIEM ของผู้รับจ้าง ตามรายการอุปกรณ์อย่างน้อยดังนี้

(1) สำหรับการนิคมอุตสาหกรรม (สำนักงานใหญ่) หรือ สำนักงานนิคมอุตสาหกรรมมาบตาพุด หรือ สำนักงานท่าเรืออุตสาหกรรมมาบตาพุด

- Active Directory จำนวน 2 ระบบ
- SDWAN Analysis จำนวน 1 ระบบ
- Antivirus Gateway จำนวน 1 เครื่อง
- Virtualization Host จำนวน 6 เครื่อง
- ERP Application Server จำนวน 1 เครื่อง
- ERP Database Server จำนวน 1 เครื่อง

(2) สำหรับศูนย์เฝ้าระวังคุณภาพสิ่งแวดล้อมและความปลอดภัย

- Active Directory จำนวน 1 เครื่อง
- DSS Server จำนวน 1 เครื่อง
- E-Monitoring Server จำนวน 1 เครื่อง
- Envista Server จำนวน 1 เครื่อง
- Emergency Online Server จำนวน 1 เครื่อง
- SDWAN Analysis จำนวน 1 ระบบ

4.4.3 ต้องดำเนินการร่วมกับเจ้าหน้าที่ กนอ. ในการตั้งค่าตามรายการอุปกรณ์ที่ใช้งานอยู่ในปัจจุบัน เพื่อให้มีการส่งข้อมูลจราจรทางคอมพิวเตอร์ (Log file) จากเครื่องและอุปกรณ์ดังกล่าวไปยังอุปกรณ์จัดเก็บข้อมูล Log ของผู้รับจ้าง

4.4.4 ติดตั้งอุปกรณ์หรือซอฟแวร์ในการจัดเก็บข้อมูล Log (Log Collector, Event Collector) ที่ การนิคมอุตสาหกรรม (สำนักงานใหญ่) หรือ ศูนย์เฝ้าระวังคุณภาพสิ่งแวดล้อมและความปลอดภัย หรือ สำนักงานนิคมอุตสาหกรรมมาบตาพุด หรือ สำนักงานท่าเรืออุตสาหกรรมมาบตาพุด ตามความเหมาะสม เพื่อจัดเก็บข้อมูล Log ส่งไปยังศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ของผู้รับจ้าง โดย กนอ. จะเป็นผู้จัดเตรียมช่องทางสื่อสาร (Internet Link) สำหรับการส่งข้อมูลดังกล่าว และจัดทำรายงานการเตรียมความพร้อมของการเฝ้าระวังภัยคุกคามทางไซเบอร์

4.4.5 ต้องสามารถวิเคราะห์เหตุการณ์ผิดปกติทางด้านบริหารจัดการระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารและอินเทอร์เน็ต เพื่อวิเคราะห์ความเกี่ยวโยงของเหตุการณ์และภัยคุกคามด้านความปลอดภัยสารสนเทศ (IT Security Monitoring) แหล่งที่มาของภัยคุกคามนั้นๆ ตลอด 24 ชั่วโมงต่อวัน 7 วันต่อสัปดาห์ (24/7)

4.4.6 ผู้รับจ้างต้องทำการเฝ้าระวัง วิเคราะห์ และแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ ผ่านทาง E-mail, โทรศัพท์ และระบบ Ticket Management ตาม Service Level Agreement และระดับความรุนแรงที่ กนอ. กำหนดดังต่อไปนี้

ระดับความรุนแรง	ผลกระทบ	เวลาในการแจ้งเตือนแก่ กนอ.	ให้คำแนะนำในการแก้ไข	ช่องทางการแจ้งเตือน
วิกฤติ (Critical)	การดำเนินธุรกิจหยุดชะงัก และจำเป็นต้องแก้ไขอย่างเร่งด่วนที่สุด	ภายใน 15 นาที	ภายใน 30 นาที	โทรศัพท์ Email Line
สูง (High)	การดำเนินธุรกิจได้รับผลกระทบมีความจำเป็นต้องแก้ไขโดยเร็ว	ภายใน 30 นาที	ภายใน 60 นาที	โทรศัพท์ Email Line
ปานกลาง (Medium)	มีผลต่อประสิทธิภาพการทำงานทั่วไป และมีผลกระทบต่อการดำเนินธุรกิจโดยภาพรวมเล็กน้อย	ภายใน 60 นาที	ภายใน 90 นาที	Email Line
ต่ำ (Low)	มีผลต่อประสิทธิภาพการทำงานทั่วไป แต่ไม่มีผลกระทบต่อการดำเนินธุรกิจโดยภาพรวม	ข้อมูลรายงาน	ข้อมูลรายงาน	สรุปรายงาน

4.4.7 การแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์ต้องครอบคลุมเนื้อหาดังต่อไปนี้

- ระบุประเภทของภัยคุกคาม
- วัน-เวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม
- ระบุต้นทาง (Attacker) และปลายทาง (Target)
- ระบุระดับความรุนแรง (Severity)
- รายละเอียดเหตุการณ์และพฤติกรรมทั้งหมด
- คำแนะนำและขั้นตอนการดำเนินการแก้ไขเชิงเทคนิค
- (ถ้ามี) ในกรณีที่เป็นเหตุการณ์ระดับ (Critical, High) ต้องมีการเขียนรายงานสรุปการแก้ไขโดยต้องสามารถบอกวิธีการ Configuration บนระบบที่ผู้ให้บริการนำเสนอ

4.4.8 จัดเก็บข้อมูล Log ของคอมพิวเตอร์เครื่องแม่ข่ายและอุปกรณ์เครือข่ายให้ครบถ้วนตามที่ กนอ. กำหนด และจัดเก็บ โดยต้องมีระยะเวลาในการจัดเก็บไม่น้อยกว่า 90 วัน และต้องดำเนินการค้นหาข้อมูลได้ทั้งหมด 30 วันแบบ Real Time เพื่อให้เป็นไปตามหลักเกณฑ์ พรบ. การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

4.4.9 ในกรณีที่ กนอ. ต้องการให้ระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ มีการจัดการรวบรวมข้อมูลจราจรทางคอมพิวเตอร์ (Log File) จากเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายงานระบบของ กนอ. ที่อยู่บน Cloud เข้าสู่ระบบวิเคราะห์ข้อมูลระบบ SIEM ของผู้รับจ้างเพิ่มเติมในกรณีที่ผู้ให้บริการ Cloud อนุญาตให้

เชื่อมต่อได้ และรองรับได้ ผู้รับจ้างจะต้องให้คำแนะนำและดำเนินการรวบรวมข้อมูลจราจรทางคอมพิวเตอร์ (Log File) จากเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายงานระบบของ กนอ. ที่อยู่บน Cloud ตามที่ กนอ. กำหนดและเห็นสมควร

4.4.10 จัดให้มีระบบบริหารจัดการ ซึ่งแสดงสถานการณ์ตรวจสอบข้อมูลความปลอดภัยของระบบเครือข่าย และข้อมูลการแจ้งเตือนและติดตามเหตุการณ์ (Ticket Management) เพื่อให้ กนอ. สามารถตรวจสอบข้อมูลได้ตลอดเวลา

4.4.11 จัดให้มีทีมงานผู้เชี่ยวชาญ เพื่อเข้าดำเนินการสืบสวนและวิเคราะห์หาสาเหตุของปัญหาภัยคุกคามที่เกิดขึ้นในความรุนแรงระดับวิกฤติ (Critical) ณ สถานที่ที่เกิดเหตุภัยคุกคามทางไซเบอร์ รวมทั้งให้คำแนะนำแนวทางการแก้ไขและป้องกันปัญหาตามที่ กนอ. ร้องขอ ไม่เกินกว่า 12 ครั้งต่อปี

4.4.12 ดำเนินการจัดทำรายงานสรุปผลการเฝ้าระวังภัยคุกคามแบบรายเดือน (Monthly Report) และรายงานข่าวสารที่เกี่ยวกับคุกคามใหม่ที่เกิดขึ้นด้านความปลอดภัยไซเบอร์ที่เกิดขึ้นทั่วโลกให้แก่ กนอ. แบบรายเดือน พร้อมนัดประชุมกับ กนอ. เพื่อสรุปภาพรวมผลการเฝ้าระวังภัยคุกคามและภัยคุกคามใหม่ ที่เกิดขึ้นและให้คำปรึกษาในการรับมือกับภัยคุกคามที่เกิดขึ้นให้ทางเจ้าหน้าที่ กนอ.

4.4.13 จัดทำรายงานผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ และสรุปผลการดำเนินการเฝ้าระวังภัยคุกคามเหตุการณ์ผิดปกติที่เป็นภัยคุกคามเป็นรายเดือน (Monthly report) โดยมีรายละเอียดดังต่อไปนี้

(1) รายงานสรุปสำหรับผู้บริหาร (Executive Summary) เพื่ออธิบายผู้บริหารให้เข้าใจสถานะความเสี่ยงและสภาพปัจจุบัน

(2) รายงานสรุปเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เกิดขึ้นโดยมีการวิเคราะห์ภัยคุกคามในเชิงลึก โดยมีเนื้อหาตามรายการดังต่อไปนี้เป็นอย่างน้อย

- Top Attackers Report
- Top Threat Report
- รายงานสรุปปริมาณการใช้งานข้อมูลจราจรทางคอมพิวเตอร์ประจำเดือน
- รายงานสรุปการแจ้งเตือนเหตุการณ์ที่ตรวจพบ (Incident Report) ประจำเดือน

4.4.14 ต้องมีการวิเคราะห์แบบรวมศูนย์และเงื่อนไขการโจมตี (Correlation and Use case) เพื่อช่วยในการเฝ้าระวังและแจ้งเตือนภัยคุกคามด้วยรูปแบบและมาตรฐานของผู้รับจ้าง อ้างอิง มาตรฐาน NIST Incident Categories เป็นอย่างน้อย

4.4.15 บริการเฝ้าระวังและแจ้งเตือนภัยคุกคามด้วยรูปแบบเงื่อนไขเฉพาะ หรือเงื่อนไขอื่นๆ เพิ่มเติมให้เหมาะสม (Custom Use case) ตามที่ กนอ. กำหนด จำนวนไม่เกิน 10 Custom Use case

4.4.16 ต้องมี Rules ที่ใช้กับอุปกรณ์เฝ้าระวัง สามารถตรวจจับเหตุการณ์การคุกคามซึ่งครอบคลุม ในเรื่องดังนี้เป็นอย่างน้อย

(1) Unauthorized Access

(2) Malicious Code

(3) Inappropriate Usage

(4) Multiple Component

(5) Denial of Service (DOS)

(6) Exercise/Network Defense Testing

4.4.17 บริการแจ้งข่าวสารซึ่งเกี่ยวข้องกับระบบรักษาความปลอดภัยทางไซเบอร์ ระบบคอมพิวเตอร์ และระบบเครือข่าย ผ่านทางอีเมล์ เช่น

(1) รายชื่อ และคุณลักษณะของมัลแวร์ (Malware)

(2) ช่องโหว่ใหม่ (Vulnerability) ของอุปกรณ์ในระบบเครือข่าย (Network Equipment)

(3) ช่องโหว่ใหม่ (Vulnerability) ของระบบปฏิบัติการ (Operating System)

(4) ช่องโหว่ใหม่ (Vulnerability) ของระบบฐานข้อมูลหลัก (Database)

(5) ช่องโหว่ใหม่ (Vulnerability) ของโปรแกรมที่ผู้รับจ้างเห็นว่าจะก่อให้เกิดผลเสียหายต่อการดำเนินงานของ กนอ.

โดยข่าวสารดังกล่าวต้องประกอบด้วยเนื้อหาที่สำคัญอย่างน้อยดังต่อไปนี้ 1) คำอธิบายทั่วไป (Overview) 2) คำอธิบายอย่างละเอียด (Description) 3) ผลกระทบ (Impact) 4) ระบบที่ได้รับผลกระทบ (System Affected) 5) การแก้ไข (Solution) (ถ้ามี) และ 6) การอ้างอิง (Reference)

4.4.18 บริการค้นหาภัยคุกคามเชิงรุก (Threat Hunting) หรือดำเนินการค้นหารูปแบบการโจมตีจาก Threat Intelligence โดยใช้เครื่องมือของผู้รับจ้าง และแจ้งเตือนให้ทราบถึงภัยคุกคามที่จะเกิดขึ้นกับ กนอ.

4.4.19 บริการแก้ไขปัญหา และจัดทำรายงานสรุปการแก้ไขปัญหาที่ได้รับแจ้งจากศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ (SOC) ของผู้รับจ้าง โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้ 1) วัน เดือน ปี ที่รับแจ้ง 2) เวลารับแจ้ง 3) ปัญหาที่ได้รับแจ้ง 4) รายงานการแก้ไขปัญหา 5) สถานะในการดำเนินการ

4.4.20 ดำเนินการประเมินความเสี่ยงจากมุมมองภายนอก (Security Rating) จำนวน 1 โดเมน ซึ่งสามารถวิเคราะห์ข้อมูลขององค์กรจากมุมมองภายนอก ที่เห็นความเสี่ยงที่อาจจะเกิดขึ้นได้ด้วยการให้คะแนนตามความเสี่ยงที่ตรวจพบ โดยระบบจะต้องประกอบด้วยการทำงาน โดยต้องประเมินความเสี่ยงตามปัจจัย (Factor) ดังนี้ Network security, DNS health, Patch, Endpoint Security, IP reputation, Application security, Public threat intelligence, Hacker chatter, Information leak, Social engineering เป็นต้น และต้องจัดส่งรายงานประจำเดือนให้กับผู้รับบริการ พร้อมจัดประชุมเพื่อให้คำแนะนำรายไตรมาส

4.4.21 จัดทำคู่มือปฏิบัติงานอัตโนมัติ (Playbook) ให้กับทาง กนอ. ปีละ 3 คู่มือปฏิบัติงานอัตโนมัติ (Playbook)

4.4.22 ต้องดำเนินการเชื่อมต่ออุปกรณ์อย่างน้อยดังต่อไปนี้ เพื่อให้ระบบเฝ้าระวังสามารถสั่งงานอัตโนมัติให้กับอุปกรณ์ต่าง ๆ ให้อย่างอัตโนมัติ

(1) Next Generation Firewall

(2) Endpoint Protection Platform

4.5 <u>การจำลองสถานการณ์การโจมตีในรูปแบบของ Social Engineering</u>

4.5.1 ออกแบบและจัดทำการทดสอบระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับพนักงาน ในรูปแบบอีเมลฟิชชิ่ง (E-Mail Phishing Awareness) โดยมีจำนวนผู้เข้ารับการทดสอบ เป็นจำนวนไม่เกิน 600 คน โดยดำเนินการทดสอบ 2 ครั้งต่อปี

4.5.2 สรุปรายงานในรูปแบบของเอกสารโดยต้องมีหัวข้อการสรุปรายงาน อย่างน้อยดังต่อไปนี้

(1) หัวข้อบทสรุปภาพรวมผู้บริหาร

(2) หัวข้อตัวอย่างที่ใช้ในการโจมตีของแต่ละรูปแบบ

(3) จำนวนผู้เปิดอีเมล

(4) จำนวนคนที่คลิกเข้าไปดูข้อมูล

(5) จำนวนบุคลากรที่รายงานว่าเป็น Phishing หรือ อีเมลแปลกปลอม โดยดำเนินการเก็บข้อมูลจากผู้รับบริการเพื่อประกอบรายงาน

(6) จำนวนภาพรวมของผู้กรอกข้อมูล

(7) รายละเอียดข้อมูลที่มีการกรอกเข้าไปในการโจมตี

4.6 <u>ดำเนินการพัฒนาแผนงาน Incident Response Plan (IRP) โดยต้องวางแนวทางปฏิบัติที่ดีที่สุดสำหรับการตอบสนองภัยคุกคาม โดยใช้สถานการณ์ข้อมูลรั่วไหล (Data Leak) จำนวน 1 แผนงาน โดยมีรายละเอียดเพิ่มเติมดังต่อไปนี้</u>

4.6.1 แผนงานยกระดับการจัดการและลำดับความสำคัญของเหตุการณ์ (Escalate matrix)

4.6.2 ขั้นตอนการรับมือเหตุการณ์ความปลอดภัยไซเบอร์ (Incident Response Workflow)

4.6.3 แผนงานการวัดประสิทธิภาพ (Performance Metric) และแผนการจัดทำรายงาน

4.6.4 ข้อกำหนดการเพิ่มระดับและการจัดการเหตุการณ์สำหรับเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Escalation and Handling) ซึ่งจำเป็นต่อการเพิ่มขีดความสามารถในการตอบสนองเหตุการณ์ความปลอดภัยไซเบอร์ของผู้รับบริการ

4.6.5 ต้องมีการจัดทำ Incident Response Playbook (IR Playbook) ซึ่งเป็นคู่มือตอบสนองต่อเหตุการณ์การโจมตีทางไซเบอร์ในแบบต่าง ๆ เป็นจำนวนอย่างน้อย 1 Playbooks โดยอาจเป็น Playbook

สำหรับรับมือกับภัยคุกคามที่ กนอ. อาจต้องเผชิญ เช่น สำหรับรับมือเหตุการณ์ Ransomware, 0-day Attack, 3rd Party Breaches เป็นต้น

4.6.6 แนวปฏิบัติการบริหารจัดการความต่อเนื่องในการดำเนินงานขององค์กรเมื่อเกิดภัยไซเบอร์

4.6.7 แนวปฏิบัติการบริหารจัดการบุคลากรที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

4.6.8 แนวปฏิบัติการบริหารจัดการด้านการสื่อสารที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

4.6.9 แนวปฏิบัติการบริหารจัดการการจัดหา การพัฒนา และการบำรุงรักษาระบบที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

4.6.10 แนวปฏิบัติการบริหารจัดการผู้ให้บริการภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

4.7 ผู้รับจ้างต้องดำเนินการจัดทำ Tabletop Exercise ตามสถานการณ์หัวข้อ 4.6 เป็นจำนวนอย่างน้อย 1 ครั้ง เพื่อประเมินความสามารถ กระบวนการและประสิทธิภาพในการตอบสนองต่อเหตุการณ์ภัยคุกคามไซเบอร์ให้แก่ผู้บริหารและหน่วยงานที่เกี่ยวข้อง

4.8 ผู้รับจ้างต้องวิเคราะห์ช่องว่างด้านความปลอดภัยทางไซเบอร์ (Gap Analysis)

4.8.1 ทบทวน บริบทขององค์กรและความต้องการของธุรกิจ เพื่อให้เข้าใจบทบาท หน้าที่ และความสามารถของการให้บริการ เพื่อให้สอดคล้องกับความต้องการของผู้เข้ามาใช้งาน และออกแบบกำหนดการรักษาความปลอดภัยให้เป็นไปตามมาตรฐานสากล

4.8.2 ดำเนินการประเมิน ความสามารถ (Capacity) และวัตถุประสงค์ (Objective) ด้านความปลอดภัยในปัจจุบันของผู้รับบริการ โดยใช้รูปแบบการรักษาความปลอดภัยที่กำหนดไว้

4.8.3 ดำเนินการตรวจสอบ วิเคราะห์ เรื่องของความปลอดภัยต่าง ๆ ขององค์กร โดยจัดทำโปรแกรมที่เน้นเรื่องของความปลอดภัย โดยใช้ CIS 18 Controls เป็นเครื่องมือในการตรวจสอบและวิเคราะห์

4.8.4 สอบถามแนวทางการปฏิบัติทั้งหมดขององค์กร และขั้นตอนการดำเนินงานต่าง ๆ ที่อาจจะทำให้เกิดช่องโหว่ หรือขั้นตอนในการอนุมัติที่จะยอมรับช่องโหว่นั้น โดยเป็นการจัดในรูปแบบการสัมภาษณ์และตรวจสอบเอกสารก่อนหน้า เพื่อประเมินและตรวจสอบ และนำไปสรุปในรูปแบบของรายงาน

4.8.5 จัดหาแนวทางการป้องกัน และช่วยให้คำแนะนำในการป้องกันช่องโหว่ต่าง ๆ ที่เกิดขึ้นในปัจจุบันและอนาคต

4.8.6 ทีมงานที่ปรึกษาสร้างแผนปฏิบัติการซึ่งรวมถึงการจัดลำดับความสำคัญของวัตถุประสงค์ที่ แนะนำแนวทางการแก้ไขปัญหาในระยะสั้นและแนวทางการแก้ไขปัญหาระยะยาว

4.8.7 การจัดทำการประเมินความเสี่ยงจะแบ่งการทำงานออกเป็น 4 ช่วงเวลา

ช่วงที่ 1 : การวางแผนการทำงาน ก่อนเริ่มดำเนินการทำงาน

- ดำเนินการประชุมหารือกับ กนอ.
- จัดส่งคำถามเบื้องต้นให้กับทาง กนอ. ตอบคำถาม
- กนอ. ดำเนินการกรอกแบบสอบถามและข้อมูลที่จำเป็นและเอกสารต่าง ๆ ที่จำเป็นที่จะใช้ในโครงการ เพื่อให้ผู้ให้บริการรับทราบถึงข้อมูลเบื้องต้น
- ผู้รับจ้างจัดให้มี ผู้บริหารจัดการโครงการ (Project Manager) ในการจัดตารางเวลาสัมภาษณ์ เพื่อพูดคุย สอบถามรายละเอียดในแบบสอบถาม และหารือถึงกระบวนการทำงานในขั้นตอนต่างๆ ด้านความปลอดภัย

ช่วงที่ 2 : สัมภาษณ์ และรวบรวมข้อมูล

- ดำเนินการสัมภาษณ์ทีมงาน กนอ.
- ดำเนินการประเมินนโยบายและมาตรฐานการรักษาความปลอดภัยของข้อมูลในปัจจุบัน เพื่อนำมาตรวจสอบและวิเคราะห์ช่องว่างตามแนวทางของ CIS 18 Controls โดยมีรายละเอียดหัวข้อที่ประเมินและวิเคราะห์ดังต่อไปนี้

01 Inventory and Control of Enterprise Assets

02 Inventory and Control of Software Assets

03 Data Protection

04 Security Configuration of Enterprise Assets and Software

05 Account Management

06 Access Control Management

07 Continuous Vulnerability Management

08 Audit Log Management

09 Email and Web Browser Protections

10 Malware Defense

11 Data Recovery

12 Network Infrastructure Management

13 Network Monitoring and Defense

14 Security Awareness and Skill Training

15 Service Provider Management

16 Application Software Security

17 Incident Response Management

18 Penetration Testing

- ดำเนินการประเมินขั้นตอนและกระบวนการรักษาความปลอดภัย เพื่อระบุระบุถึงช่องว่าง (Gap Analysis) ที่ใช้ในการตอบสนองต่อเหตุการณ์ด้านความปลอดภัย การเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลที่เป็นความลับ และข้อควรพิจารณาเกี่ยวกับแนวปฏิบัติอื่น ๆ ขององค์กร

ช่วงที่ 3 : วิเคราะห์และจัดเตรียมรายงาน

- ดำเนินการตรวจสอบและวิเคราะห์ความสามารถในการรักษาความปลอดภัยปัจจุบันของ กนอ. และเปรียบเทียบกับการวิเคราะห์เดิม ดูถึงความแตกต่างที่เกิดขึ้น
- ดำเนินการเขียนคำแนะนำเกี่ยวกับขอบเขต และการกำหนดค่าของนโยบายและการควบคุมขั้นตอนต่าง ๆ เพื่อปิดช่องว่างที่เกิดขึ้นในองค์กร

ช่วงที่ 4 : จัดทำรายงานสรุป

- ผู้รับจ้างดำเนินการตรวจสอบและวิเคราะห์ความคิดเห็นของผู้ใช้ปลายทางเกี่ยวกับรายงานการประเมินความเสี่ยง
- ผู้รับจ้างส่งมอบเอกสารขั้นสุดท้าย
- ผู้รับจ้างจัดการประชุมเพื่อนำเสนอข้อแนะนำต่าง ๆ ตามที่ระบุในเอกสาร

4.9 ผู้รับจ้างต้องดำเนินการจัดหาและติดตั้งระบบตรวจจับและตอบสนองต่อภัยคุกคามสำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (Endpoint Detection and Response : EDR) จำนวนไม่น้อยกว่า 700 Clients และ 50 Servers โดยมีคุณลักษณะอย่างน้อยดังนี้

4.9.1 เป็นระบบที่สามารถตรวจจับและป้องกันภัยคุกคามที่โจมตีบนเครื่องคอมพิวเตอร์ปลายทาง จากภัยคุกคามต่าง ๆ ได้ เช่น Ransomware, Unknown Malware, Exploit, Lateral Movement and Trojans ได้เป็นอย่างน้อย

4.9.2 ระบบที่เสนอต้องมีความสามารถในการตรวจจับและป้องกันภัยคุกคามได้แม้เครื่องคอมพิวเตอร์ปลายทางขาดการเชื่อมต่อ (Offline)

4.9.3 สามารถติดตั้ง Agent บนระบบปฏิบัติการของเครื่องคอมพิวเตอร์ปลายทางได้เป็นอย่างน้อยดังนี้ Window7 SP1, Window 8 หรือ Windows 8.1, Window 10, Windows Sever, Linux และ Mac OS รวมถึงสามารถป้องกันการถอนการติดตั้งโปรแกรมได้

4.9.4 สามารถทำ Full Disk Scan ผ่านหน้าบริหารการจัดการ เพื่อค้นหา Malware หรือตรวจสอบว่าภัยคุกคามที่เกิดขึ้น ได้รับการแก้ไขแล้ว

4.9.5 สามารถแสดงเหตุการณ์ที่ถูกภัยคุกคามโจมตี เช่น ไฟล์ที่ถูกภัยคุกคามสร้างขึ้น (File Creation), ไฟล์ที่ถูกภัยคุกคามแก้ไข (File Modification), ไฟล์ที่ถูกภัยคุกคามลบ (File Deletion), Network Actions, ข้อมูล Process เป็นต้น

4.9.6 สามารถแสดงผล Process Tree หรือตารางของเหตุการณ์ที่ถูกภัยคุกคามโจมตี เพื่อวิเคราะห์หลังการดำเนินการ (Execution)

4.9.7 สามารถสั่งแยกเครื่องคอมพิวเตอร์ที่มีความเสี่ยงจากภัยคุกคามออกจากระบบเครือข่าย (Disconnect or Isolate from Network) เพื่อป้องกันและควบคุมการแพร่กระจายของมัลแวร์ได้ รวมถึงสามารถเรียกสถานะการเชื่อมต่อคืนได้ (Reconnect or Restore to Network) ผ่านหน้าบริหารการจัดการ

4.9.8 ระบบสามารถทำงานควบคุม Network Connectivity หรือ Firewall Control หรือ Micro-Segmentation เพื่อควบคุมการเชื่อมต่อของคอมพิวเตอร์ปลายทางได้

4.9.9 สามารถควบคุมการใช้งานอุปกรณ์ Removable Media หรือ USB control

4.9.10 ระบบสามารถแสดงรายการช่องโหว่ โดยสามารถรองรับ MITRE CVE database ได้ หรือสามารถป้องกันช่องโหว่ของ Software ได้ (Exploit Protection)

4.9.11 ระบบสามารถควบคุมดำเนินการเครื่องคอมพิวเตอร์ปลายทางจากศูนย์กลางได้ หลังการถูกโจมตี เช่น Kill Process, Quarantine, Delete file และ การเปลี่ยนแปลงของระบบที่ถูกสร้างขึ้นโดยมัลแวร์

4.9.12 ระบบสามารถทำ Threat Hunting เพื่อเป็นเครื่องมือให้ Security Team ในการค้นหาภัยคุกคามเชิงรุกจากตัวบ่งชี้ภัยคุกคาม Indicators of Compromise (IOC) และพฤติกรรมของผู้โจมตี โดยสามารถสืบค้นหาพฤติกรรมของการโจมตีหรือภัย คุกคาม เข้ากับ MITRE ATT&CK Framework ได้

4.9.13 สามารถทำการเก็บหลักฐานการโจมตีที่เกิดขึ้นบนเครื่องคอมพิวเตอร์ปลายทางเพื่อตรวจสอบย้อนหลังได้ไม่น้อยกว่า 14 วัน สำหรับค่าต่าง ๆ ในการค้นหา เช่น Host name, OS, Domain Name, IP address และ Process ได้เป็นอย่างน้อย

4.10 <u>บริการตอบสนองต่อภัยคุกคามสำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (Managed Detection and Response: MDR)</u> โดยมีรายละเอียดการให้บริการดังต่อไปนี้

4.10.1 เมื่อมีเหตุการณ์ภัยคุกคามที่เป็นอัตรายเกิดขึ้นผู้ให้บริการต้องดำเนินการหยุดกระบวนการที่เป็นอันตราย โดยต้องดำเนินการอย่างน้อยดังต่อไปนี้

(1) ทำความเข้าใจเกี่ยวกับขอบเขตของผลกระทบ และการแพร่กระจายของภัยคุกคาม

(2) แยก Endpoint ที่เป็นอันตรายออกจากระบบในกรณีที่วิเคราะห์ได้ว่าอาจมีการแพร่กระจายไปสู่ Endpoint เครื่องอื่นๆ ในระบบ

(3) ระงับ ยับยั้ง หรือ ยุติกระบวนการที่เป็นอันตรายต่อระบบ

(4) ลบ/ล้างแอปพลิเคชันและไฟล์ที่เกี่ยวข้องกับเหตุการณ์ภัยคุกคามในกรณีที่เครื่อง Endpoint ได้รับผลกระทบจะต้องดำเนินการกู้คืนกลับมาสู่สภาพที่พร้อมใช้งานได้ (โดยข้อจำกัดและเงื่อนไขของซอฟต์แวร์จำพวก EDR หรือ XDR หรือสถานะของเครื่อง Endpoint)

4.10.2 บริการให้คำแนะนำเกี่ยวกับเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ถูกตรวจพบโดยซอฟต์แวร์จำพวก EDR หรือ XDR ซึ่งถูกใช้เพื่อให้บริการในการป้องกัน เฝ้าระวังและตอบสนอง

4.10.3 สรุปรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อเครื่อง Endpoint (Threat Incident Report) โดยจะต้องมีรายละเอียดรายงานอย่างน้อยดังต่อไปนี้

(1) Executive Summary (สรุปสาระสำคัญของเหตุการณ์ภัยคุกคาม)

(2) Incident/Alarm Detail (รายละเอียดเหตุการณ์ภัยคุกคาม)

(3) Impact Data หรือ Impact analysis (ข้อมูลภายในที่ได้รับผลกระทบจากเหตุการณ์ภัยคุกคาม)

(4) Business Risk หรือ Risk Index (ความเสี่ยงทางธุรกิจจากเหตุการณ์ภัยคุกคาม)

(5) Root Cause Analysis (วิเคราะห์สาเหตุของเหตุการณ์ภัยคุกคาม)

(6) Recommendation (คำแนะนำในการแก้ไขเหตุการณ์ภัยคุกคาม)

4.10.4 บริการรายงานสรุปสถิติภัยคุกคามประจำวัน (Daily Summary Report) โดยจะต้องมีเนื้อหาดังต่อไปนี้

(1) Top 3 Hosts by Most Alerts หรือ Top Endpoints with Detections

(2) Top 3 Threat Signatures หรือ Overall Threat summary

(3) Overall Endpoint Status หรือ Endpoint Inventory

(4) Total Incident by Severity หรือ Workbench Alert Overview

(5) Total Incident by Status หรือ Workbench Alert Tracking

(6) Detections by MITRE ATT&CK Tactics หรือ MITER ATT&CK Mapping for Enterprise

(7) Total Incident Action หรือ Virus/Malware Action/Result Summary

(8) Incident Detail หรือ Incident View

4.10.5 บริการรายงานสรุปสถิติภัยคุกคามประจำเดือน (Monthly Report) โดยสรุปเหตุการณ์ประจำเดือน

4.10.6 บริการเข้าร่วมประชุมประจำเดือน ทั้งแบบประชุมทางไกล (Video Conference Monthly Meeting) หรือเข้าประชุม ณ. ที่ กนอ. (On-Site Monthly Meeting) โดยผู้รับจ้างจะต้องเข้าร่วม

ประชุมเพื่อสรุปผลงานบริการวิเคราะห์เฝ้าระวังภัยคุกคามต่าง ๆ ที่เกิดขึ้นกับผู้รับบริการ ทุก ๆ เดือน ตลอดสัญญาของการให้บริการ

4.10.7 จัดให้มีบริการแจ้งข่าวสารซึ่งเกี่ยวข้องกับระบบรักษาความมั่นคงปลอดภัย ระบบคอมพิวเตอร์และระบบเครือข่ายที่เกิดขึ้น ผ่านทางอีเมล์

4.10.8 เสนอบริการตรวจจับภัยคุกคามและการโจมตีเชิงรุก (Threat Hunting) จากระบบข่าวกรองภัยคุกคามไซเบอร์โดยครอบคลุมทุกเครื่องคอมพิวเตอร์ลูกข่ายที่ติดตั้งซอฟต์แวร์จำพวก EDR หรือ XDR

4.10.9 เสนอบริการการจัดการตัวบ่งชี้การโจมตีทางไซเบอร์ Indicator of Attack (IOA) และตัวบ่งชี้การบุกรุกทางไซเบอร์ Indicator of Compromise (IOC) จากระบบข่าวกรองภัยคุกคามไซเบอร์ โดยครอบคลุมทุกเครื่องคอมพิวเตอร์ลูกข่ายที่ติดตั้งซอฟต์แวร์จำพวก EDR หรือ XDR

4.10.10 เสนอบริการการแจ้งเตือนความพร้อมของเซนเซอร์ (Sensor Health) ของซอฟต์แวร์จำพวก EDR หรือ XDR ในกรณีที่เครื่อง Endpoint ขาดการติดต่อกับคอนโซลของ EDR หรือ XDR

4.10.11 เสนอบริการเพิ่มการตรวจจับภัยคุกคามตามที่ผู้รับบริการให้ความสนใจตามบริบท บนซอฟต์แวร์จำพวก EDR หรือ XDR

4.10.12 แจ้งเตือนภัยคุกคามทางไซเบอร์ สำหรับเหตุการณ์ที่อยู่ในขอบข่ายภัยคุกคามทางไซเบอร์ โดยจะต้องแจ้งเตือนผ่านทาง Email หรือทางโทรศัพท์ หรือช่องทางอื่นใด ตามที่จะตกลงร่วมกันกับ กนอ. ตาม Severity Level Agreement (SLA) อย่างน้อยดังต่อไป ดังนี้

ระดับความรุนแรง	เงื่อนไขการตรวจสอบ	ดำเนินการวิเคราะห์เหตุการณ์ (หลังจากได้รับการแจ้งเตือนจาก EDR หรือ XDR)	แจ้งเตือนผู้รับบริการ	ให้คำแนะนำในการแก้ไข
วิกฤติ (Critical)	พบพฤติกรรมที่เป็น Critical หรือการแจ้งเตือนที่เป็น Critical จำนวน 1 ครั้ง	ภายใน 10 นาที	ภายใน 20 นาที หลังจากดำเนินการวิเคราะห์เหตุการณ์แล้วเสร็จ	ภายใน 60 นาที หลังจากดำเนินการแจ้งเตือนผู้รับบริการแล้วเสร็จ
สูง (High)	พบพฤติกรรมที่เป็น High หรือการแจ้งเตือนที่เป็น High จำนวน 1 ครั้ง	ภายใน 30 นาที	ภายใน 30 นาที หลังจากดำเนินการวิเคราะห์เหตุการณ์แล้วเสร็จ	ภายใน 90 นาที หลังจากดำเนินการแจ้งเตือนผู้รับบริการแล้วเสร็จ
กลาง (Medium)	พบพฤติกรรมที่เป็น Medium หรือการแจ้งเตือนที่เป็น Medium ภายในเครื่องเดิม เป็นจำนวนมากกว่า 3 ครั้ง	ภายใน 60 นาที	ภายใน 90 นาที หลังจากดำเนินการวิเคราะห์เหตุการณ์แล้วเสร็จ	ภายใน 180 นาที หลังจากดำเนินการแจ้งเตือนผู้รับบริการแล้วเสร็จ
ต่ำ (Low)	พบพฤติกรรมที่เป็น Low หรือการแจ้งเตือนที่เป็น Low ภายในเครื่องเดิม เป็นจำนวนมากกว่า 10 ครั้ง	ภายใน 120 นาที	ภายใน 180 นาที หลังจากดำเนินการวิเคราะห์เหตุการณ์แล้วเสร็จ	ภายใน 360 นาทีหลังจากดำเนินการแจ้งเตือนผู้รับบริการแล้วเสร็จ

4.11 <u>บริการระบบป้องกันการโจมตีทางเว็บไซต์ (Web Application Firewall)</u> จำนวน 1 Domain มีความสามารถขั้นต่ำอย่างน้อยดังนี้

4.11.1 สามารถป้องกันการโจมตีผ่านทาง Website ตาม OWASP TOP 10 เช่น SQL injection, Broken Authentication, Cross-site Scripting ได้

4.11.2 สามารถตั้งค่า Web Application Firewall (WAF) และสามารถแก้ไข เพิ่ม Custom WAF rules ได้ไม่น้อยกว่า 100 rules

4.11.3 สามารถป้องกันการโจมตีจากในระดับเครือข่าย (DDoS Attack) ที่ระดับ Network layer 3, 4 และ 7

4.11.4 สามารถตั้งค่า IP Firewall โดยสามารถกำหนดเงื่อนไขด้วย IP address, IP address range, Autonomous System Number (ASN) or country ได้

4.11.5 สามารถตั้งค่า Rate Limit Rules ซึ่งสามารถกำหนดการป้องกันการเข้าถึง Website ได้ในระดับ Unique Visitor

4.11.6 สามารถตั้งค่า Page Rules หรือ CND Rules ได้ไม่น้อยกว่า 100 rules

4.11.7 ผู้รับจ้างต้องให้บริการ Authoritative DNS Services สำหรับโดเมนสาธารณะ

4.11.8 มีระบบ Content Caching โดยสามารถทำ Static Content Caching และสามารถกำหนด Cache ในระดับ File Type ได้

4.11.9 สามารถทำการ Purge Cache ทั้งหมดได้ในทันที หรือทำการ Custom Purge เฉพาะ URL, Host name และ Tag ได้

4.11.10 มีระบบที่ช่วยเพิ่มประสิทธิภาพหรือลด Latency ให้กับ Dynamic Content โดยสามารถดูเปอร์เซ็นต์ของประสิทธิภาพที่เพิ่มขึ้นหรือ Response time ได้ผ่านทาง Dashboard

4.11.11 มีระบบ Always Online ที่สามารถทำการแสดง static content ในกรณีที่ Server ต้นทางไม่สามารถใช้งานได้

4.11.12 ผู้รับจ้างต้องมีเครือข่ายที่มีความสามารถในการป้องกันการโจมตีจากในระดับเครือข่าย (DDoS) ขนาด 50 Tbps เป็นอย่างน้อย

4.11.13 บริการที่เสนอรองรับการส่ง Raw Log ผ่านทาง Log Push ไปยัง Amazon S3, Azure Blob Storage, Google Cloud Storage, or Sumo Logic ได้เป็นอย่างน้อย

4.11.14 สามารถเรียกดู Firewall Event Log หรือ Audit Log ได้ผ่านทาง Portal ที่ใช้งาน

4.11.15 บริการที่เสนอต้องรองรับการกำหนดสิทธิเข้าใช้งาน หรือรองรับการทำ Two-Factor Authentication ได้

4.11.16 บริการที่เสนอต้องสามารถรองรับการใช้ Bandwidth Consumption ได้ไม่น้อยกว่า 1 TB ต่อเดือน

4.11.17 บริการที่นำเสนอต้องมีสิทธิ์การใช้งานได้ไม่น้อยกว่า 1 domain และต้องใช้งานได้ไม่น้อยกว่า 5 Sub - Domain และต้องไม่มีการจำกัดจำนวน Application

4.11.18 รองรับการติดตั้งทั้งแบบการย้าย Name Server หรือ CNAME ได้

4.11.19 สามารถทำการวิเคราะห์และแยกแยะบอทและมนุษย์โดยใช้เทคนิค Heuristics, Machine Learning (ML) และ JavaScript Detections (JSD) ได้เป็นอย่างน้อย

4.11.20 สามารถแสดงรายละเอียดเกี่ยวกับสคริปต์ที่ตรวจพบบนหน้าเว็บเพจได้ว่าถูกเพิ่มมาเมื่อไร และอยู่ที่ URL ไหนบนหน้าเว็บเพจ หรือ สามารถค้นหา API (API Discovery) และยับยั้งการโจมตี API (API Mitigation) ได้อย่างอัตโนมัติ

4.12 <u>การจัดฝึกอบรม</u>

4.12.1 ดำเนินการจัดอบรมหลักสูตรการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ สำหรับผู้บริหารระดับสูง เจ้าหน้าที่ฝ่ายดิจิทัล ซึ่งจะเป็นการบรรยายเป็นจำนวน 1 ครั้ง ระยะเวลา 3 ชั่วโมง จำนวนผู้รับการอบรมไม่น้อยกว่า 20 คน หรือตามที่ กนอ. กำหนดเพิ่มเติม โดยผู้รับจ้างต้องส่งรายละเอียดการอบรมให้ กนอ. พิจารณา ก่อนเริ่มการอบรม โดยมีหัวข้อดังต่อไปนี้

(1) การสร้างวัฒนธรรมที่ตระหนักรู้ด้านความเสี่ยงไซเบอร์ภายในองค์กร
(2) ภัยคุกคามไซเบอร์รูปแบบต่าง ๆ
(3) การสร้างความสามารถในการเฝ้าระวังให้กับองค์กร
(4) ความเข้าใจด้านการป้องกันจุดอ่อนในเชิงนโยบาย
(5) ความสำคัญของการจัดการในการรับมือกับอุบัติการณ์
(6) การป้องกันปัญหาการรั่วไหลของข้อมูล
(7) มาตรฐาน ISO27001

4.12.2 ดำเนินการจัดอบรมหลักสูตรการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ใช้งานคอมพิวเตอร์ทั่วไป ซึ่งจะเป็นการบรรยายเป็นจำนวน 1 ครั้ง ระยะเวลา 3 ชั่วโมง จำนวนผู้รับการอบรมไม่น้อยกว่า 100 คน หรือตามที่ กนอ. กำหนดเพิ่มเติม โดยผู้รับจ้างต้องส่งรายละเอียดการอบรมให้ กนอ. พิจารณา ก่อนเริ่มการอบรม โดยมีหัวข้อดังต่อไปนี้

(1) ความหมายของความมั่นคงปลอดภัยต่อตัวบุคคลและองค์กร
(2) จุดประสงค์ของการจัดการความมั่นคงปลอดภัย และประโยชน์ของการปฏิบัติตามนโยบาย
(3) การโจมตีช่องโหว่ต่าง ๆ ที่เกิดขึ้นจากความไม่ตระหนักรู้
(4) การใช้รหัสผ่านอย่างถูกต้องและผลร้ายของการใช้ที่ไม่ถูกต้อง
(5) สิ่งที่ควรรู้เกี่ยวกับคอมพิวเตอร์ไวรัส
(6) กฎหมายเรื่องอาชญากรรมคอมพิวเตอร์ที่ควรรู้

4.12.3 จัดให้มีการฝึกอบรมและแนะนำการใช้งานระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ และระบบตรวจจับและตอบสนองต่อภัยคุกคาม ระยะเวลาไม่เกิน 6 ชั่วโมง สำหรับผู้ดูแลระบบ (Administrator) โดยรองรับผู้เข้ารับการอบรมจำนวน ไม่น้อยกว่า 10 คน พร้อมจัดส่งคู่มือการใช้งาน

4.12.4 ผู้รับจ้างต้องจัดให้มีการฝึกอบรมภายในประเทศพร้อมสอบใบรับรองความสามารถหลักสูตรประกาศนียบัตรผู้เชี่ยวชาญระบบความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ CompTIA : Security+ หรือหลักสูตรตามที่ กนอ. เห็นชอบ จากหน่วยงานเจ้าของมาตรฐานหรือตัวแทนที่ได้รับการแต่งตั้ง จำนวน 2 คน

4.12.5 ผู้รับจ้างต้องจัดให้มีการฝึกอบรมภายในประเทศพร้อมสอบใบรับรองความสามารถหลักสูตรประกาศนียบัตรผู้เชี่ยวชาญระบบความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ CompTIA : CySA+ หรือหลักสูตรตามที่ กนอ. เห็นชอบ จากหน่วยงานเจ้าของมาตรฐานหรือตัวแทนที่ได้รับการแต่งตั้ง จำนวน 2 คน

ทั้งนี้ ผู้รับจ้างเป็นผู้รับผิดชอบค่าใช้จ่ายเกี่ยวกับฝึกอบรม เอกสารประกอบการฝึกอบรม อาหารและอาหารว่าง เป็นต้น รวมทั้งค่าธรรมเนียมหลักสูตร (ถ้ามี)

4.13 <u>บุคลากรในโครงการ</u>

เพื่อให้การบริการตามขอบเขตของงานด้วยคุณภาพประสิทธิภาพตลอดระยะเวลาบริการ ผู้รับจ้างต้องจัดให้มีบุคลากรตำแหน่งต่าง ๆ ที่กำหนดใน **ภาคผนวก ก** โดยให้ระบุชื่อ ตำแหน่ง หน้าที่รับผิดชอบให้ชัดเจน พร้อมแนบเอกสารประวัติบุคคลแสดงวุฒิการศึกษา ประสบการณ์การทำงาน ใบรับรองความรู้ความสามารถจำนวนและคุณสมบัติของบุคลากร

5. ระยะเวลาดำเนินงาน

ภายในระยะเวลาดำเนินงานทั้งสิ้น 420 วันนับถัดจากวันลงนามในสัญญา

6. วงเงินงบประมาณ

ภายในวงเงินงบประมาณทั้งสิ้น 7,600,000 บาท (เจ็ดล้านหกแสนบาทถ้วน) ซึ่งรวมภาษีมูลค่าเพิ่ม และค่าใช้จ่ายทั้งปวงไว้เรียบร้อยแล้ว โดยเบิกจ่ายจากเงินงบประมาณประจำปี 2567

7. งวดการส่งมอบงานและงวดการจ่ายเงิน

กนอ. จะจ่ายค่าจ้างบริการศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์และทดสอบความมั่นคงปลอดภัยของระบบสารสนเทศ กนอ. ประจำปี 2566 – 2567 โดยแบ่งจ่ายเป็นงวด รวม 5 งวด เมื่อผู้รับจ้างให้บริการตามข้อ 4.4 และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว โดยมีรายละเอียดการส่งมอบบริการแต่ละงวด ดังนี้

7.1 <u>งวดงานที่ 1</u>

จ่ายค่าจ้างบริการร้อยละ 40 ของค่าจ้างตามสัญญา เมื่อผู้รับจ้างจะต้องส่งมอบผลการดำเนินงานภายใน 60 วันนับถัดจากวันลงนามในสัญญา ประกอบด้วย

(1) แผนการดำเนินงานตลอดระยะเวลาของโครงการตามขอบเขตของงาน ข้อ 4.1

(2) รายงานผลการตรวจสอบช่องโหว่ (VA) พร้อมการวิเคราะห์และจัดทำข้อเสนอแนะ ครั้งที่ 1 ตามขอบเขตของงาน ข้อ 4.2.1 และ 4.2.2

(3) รายงานผลการปิดช่องโหว่ตามผลการตรวจสอบช่องโหว่ (VA) ครั้งที่ 1 ตามขอบเขตของงาน ข้อ 4.2.3

(4) รายงานผลการทดสอบเจาะระบบ (Penetration Testing) พร้อมการวิเคราะห์และจัดทำข้อเสนอแนะ ครั้งที่ 1 ตามขอบเขตของงาน ข้อ 4.3.1 และ 4.3.2

(5) รายงานผลการติดตั้งอุปกรณ์จัดเก็บข้อมูล Log และรายงานผลการตั้งค่าระบบวิเคราะห์และจัดการข้อมูลจราจรด้านความปลอดภัยสำหรับให้บริการเฝ้าระวังภัยคุกคามแก่ กนอ. ตามขอบเขตของงาน ข้อ 4.4.4

(6) รายงานผลการทดสอบจำลองอีเมล Phishing ด้วยรูปแบบเหตุการณ์เสมือน ครั้งที่ 1 ตามขอบเขตของงาน ข้อ 4.5

(7) ผู้รับจ้างจะต้องส่งมอบ License ระบบ EDR ตามข้อ 4.10 และ License ระบบ WAF ตามขอบเขตของงาน ข้อ 4.12

(8) ผู้รับจ้างต้องจัดให้มีการฝึกอบรมและแนะนำการใช้งานระบบตามขอบเขตของงาน ข้อ 4.12.3

7.2 <u>งวดงานที่ 2</u>

จ่ายค่าจ้างบริการร้อยละ 15 ของค่าจ้างตามสัญญา เมื่อผู้รับจ้างจะต้องส่งมอบผลการดำเนินงานภายใน 150 วันนับถัดจากวันลงนามในสัญญา ประกอบด้วย

(1) รายงานผลการตรวจสอบช่องโหว่ (VA) พร้อมการวิเคราะห์และจัดทำข้อเสนอแนะ ครั้งที่ 2 ตามขอบเขตของงาน ข้อ 4.2.4 และ 4.2.5

(2) รายงานผลการปิดช่องโหว่ตามผลการตรวจสอบช่องโหว่ (VA) ครั้งที่ 2 ตามขอบเขตของงาน ข้อ 4.2.6

(3) รายงานผลการทดสอบเจาะระบบ (Penetration Testing) พร้อมการวิเคราะห์และจัดทำข้อเสนอแนะ ครั้งที่ 2 ตามขอบเขตของงาน ข้อ 4.3.3 และ 4.3.4

(4) รายงานผลการทดสอบจำลองอีเมล Phishing ด้วยรูปแบบเหตุการณ์เสมือน ครั้งที่ 2 ตามขอบเขตของงาน ข้อ 4.5

(5) รายงานสรุปผลการเฝ้าระวังภัยคุกคามด้วยศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ตามขอบเขตของงาน ข้อ 4.4.12 ประจำเดือนที่ 1-3

(6) รายงานสรุปผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ตามขอบเขตของงาน ข้อ 4.4.13 ประจำเดือนที่ 1-3

(7) รายงานสรุปผลการตอบสนองต่อภัยคุกคามสำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (MDR) ตามขอบเขตของงาน ข้อ 4.10 ประจำเดือนที่ 1-3

(8) จัดอบรมหลักสูตรการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศตามขอบเขตของงาน ข้อ 4.12.1 และ 4.12.2

(9) รายงานสรุปการจัดทำ Incident Response Plan ตามขอบเขตของงาน ข้อ 4.6

(10) รายงานสรุปการจัดทำ Tabletop Exercise ตามขอบเขตของงาน ข้อ 4.7

(11) รายงานสรุปบทวิเคราะห์ช่องว่างด้านความปลอดภัยทางไซเบอร์ (GAP Analysis) ตามขอบเขตของงาน ข้อ 4.8

7.3 งวดงานที่ 3

จ่ายค่าจ้างบริการร้อยละ 15 ของค่าจ้างตามสัญญา เมื่อผู้รับจ้างจะต้องส่งมอบผลการดำเนินงานภายใน 240 วันนับถัดจากวันลงนามในสัญญา ประกอบด้วย

(1) รายงานสรุปผลการเฝ้าระวังภัยคุกคามด้วยศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ตามขอบเขตของงาน ข้อ 4.4.12 ประจำเดือนที่ 4-6

(2) รายงานสรุปผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ตามขอบเขตของงาน ข้อ 4.4.13 ประจำเดือนที่ 4-6

(3) รายงานสรุปผลการตอบสนองต่อภัยคุกคามสำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (MDR) ตามขอบเขตของงาน ข้อ 4.10 ประจำเดือนที่ 4-6

7.4 งวดงานที่ 4

จ่ายค่าจ้างบริการร้อยละ 15 ของค่าจ้างตามสัญญา เมื่อผู้รับจ้างจะต้องส่งมอบผลการดำเนินงานภายใน 330 วันนับถัดจากวันลงนามในสัญญา ประกอบด้วย

(1) รายงานสรุปผลการเฝ้าระวังภัยคุกคามด้วยศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ตามขอบเขตของงาน ข้อ 4.4.12 ประจำเดือนที่ 7-9

(2) รายงานสรุปผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ตามขอบเขตของงาน ข้อ 4.4.13 ประจำเดือนที่ 7-9

(3) รายงานสรุปผลการตอบสนองต่อภัยคุกคามสำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (MDR) ตามขอบเขตของงาน ข้อ 4.10 ประจำเดือนที่ 7-9

7.5 งวดงานที่ 5 (งวดสุดท้าย)

จ่ายค่าจ้างบริการร้อยละ 15 ของค่าจ้างตามสัญญา เมื่อผู้รับจ้างจะต้องส่งมอบผลการดำเนินงานภายใน 420 วันนับถัดจากวันลงนามในสัญญา ประกอบด้วย

(1) รายงานสรุปผลการเฝ้าระวังภัยคุกคามด้วยศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ตามขอบเขตของงาน ข้อ 4.4.12 ประจำเดือนที่ 10-12

(2) รายงานสรุปผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ตามขอบเขตของงาน ข้อ 4.4.13 ประจำเดือนที่ 10-12

(3) รายงานสรุปผลการตอบสนองต่อภัยคุกคามสำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (MDR) ตามขอบเขตของงาน ข้อ 4.10 ประจำเดือนที่ 10-12

(4) จัดให้มีการฝึกอบรมภายในประเทศพร้อมสอบใบรับรองความสามารถหลักสูตรตามขอบเขตของงาน ข้อ 4.12.4 และ 4.12.5

8. ค่าปรับ

8.1 การจ้างบริการศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์และทดสอบความมั่นคงปลอดภัยของระบบสารสนเทศ กนอ. ประจำปี 2566 – 2567 กนอ. ต้องการความสำเร็จในแต่ละงวดงานที่กำหนดในข้อ 7 หากผู้รับจ้างไม่สามารถส่งมอบงานแต่ละงวดภายในระยะเวลาที่กำหนด จะต้องยินยอมให้ กนอ. ปรับเป็นรายวันในอัตราร้อยละ 0.20 ของค่าจ้างบริการแต่ละงวด นับแต่วันครบกำหนดการส่งมอบงานจนถึงวันที่ส่งมอบงานครบถ้วนถูกต้อง

8.2 นอกจากค่าปรับตามข้อ 8.1 แล้ว ผู้รับจ้างต้องชำระค่าปรับเพิ่มเกี่ยวกับคุณภาพประสิทธิภาพการบริการ ในกรณีต่าง ๆ ดังนี้

8.2.1 กรณีผู้รับจ้างไม่ปฏิบัติตามหรือไม่สามารถให้บริการได้ตามข้อตกลงระดับการบริหาร (Service Level Agreement) ที่ กนอ. กำหนดตามข้อ 4.4.6 และข้อ 4.10.12 ผู้รับจ้างต้องชำระค่าปรับเป็นรายชั่วโมงในอัตราร้อยละ 0.025 ของราคาค่าจ้างทั้งหมดตามสัญญา เศษของชั่วโมงให้นับเป็น 1 ชั่วโมง

8.2.2 กรณีผู้รับจ้างไม่สามารถซ่อมแซมแก้ไขให้ระบบ EDR ตามข้อ 4.9 สามารถกลับมาใช้งานได้ดีดังเดิม ภายในเวลาไม่เกิน 7 วันทำการ นับถัดจากวันที่ได้รับแจ้งความชำรุดบกพร่อง กนอ. จะปรับเป็นรายชั่วโมงในอัตราร้อยละ 0.025 ของราคาค่าจ้างทั้งหมดตามสัญญา เศษของชั่วโมงให้นับเป็น 1 ชั่วโมง

8.2.3 กรณีผู้รับจ้างไม่สามารถซ่อมแซมแก้ไขให้ระบบ WAF ตามข้อ 4.11 สามารถกลับมาใช้งานได้ดีดังเดิม ภายในเวลาไม่เกิน 7 วันทำการ นับถัดจากวันที่ได้รับแจ้งความชำรุดบกพร่อง กนอ. จะปรับเป็นรายชั่วโมงในอัตราร้อยละ 0.025 ของราคาค่าจ้างทั้งหมดตามสัญญา เศษของชั่วโมงให้นับเป็น 1 ชั่วโมง

8.3 ค่าปรับตามข้อ 8.1 – 8.2 กนอ. จะหักจากค่าจ้างบริการที่ต้องจ่ายในแต่ละงวดที่เกิดค่าปรับ หากค่าจ้างบริการไม่เพียงพอหักค่าปรับ กนอ. จะหักเอาจากค่าจ้างบริการงวดต่อไปจนครบจำนวนค่าปรับนั้น

9. การยื่นข้อเสนอ

ผู้ยื่นข้อเสนอต้องยื่นเอกสารประกอบการพิจารณาที่เกี่ยวข้อง โดยต้องจัดทำเอกสารข้อเสนอตามรายการและรายละเอียดที่กำหนดในเอกสารประกวดราคาอิเล็กทรอนิกส์ หรือหนังสือเชิญชวนแล้วแต่กรณี พร้อมทั้งต้องจัดทำเอกสารข้อเสนอเพิ่มเติมนอกเหนือจากที่กำหนดไว้ ดังนี้

9.1 เอกสารตารางเปรียบเทียบข้อเสนอกับขอบเขตของงานที่ กนอ. กำหนดทุกรายการ เพื่อแสดงการยอมรับตามข้อกำหนด ข้อเปรียบเทียบดีกว่าหรือเทียบเท่า สำหรับรายละเอียดคุณลักษณะของครุภัณฑ์ต้องระบุยี่ห้อและรุ่นไว้อย่างชัดเจน และให้ระบุเลขหน้าของเอกสารแคตตาล็อก ไว้ในช่องเอกสารอ้างอิง (ระบุเลขหน้า)

9.2 เอกสารแคตตาล็อกของระบบ EDR หรือ WAF หรือรายการอื่นๆ ที่เกี่ยวข้องในโครงการ เป็นเอกสารภาษาไทยและ/หรือภาษาอังกฤษ ที่จัดทำขึ้นโดยผู้ผลิตที่เสนอมาเท่านั้น ทั้งนี้ สามารถพิมพ์แคตตาล็อกที่ถูกจัดทำไว้ในเว็บไซต์ของผู้ผลิตได้ เอกสารแคตตาล็อกทั้งหมดต้องจัดเรียงและกำหนดเลขหน้าให้ชัดเจน โดยให้ขีดเส้นใต้และเขียนเลขหัวข้อตามคุณลักษณะ หากมีรายการคุณลักษณะใดที่ไม่ปรากฏในแคตตาล็อก ต้องมีหนังสือรับรองจากผู้ผลิตรับรองคุณลักษณะดังกล่าวไว้อย่างชัดเจน โดยแนบต่อท้ายแคตตาล็อกของแต่ละรายการ

9.3 การเสนอคุณลักษณะที่เทียบเท่าหรือดีกว่าในรายการครุภัณฑ์ที่เสนอมาข้างต้น ในกรณีที่เสนอคุณลักษณะไม่ตรงตามที่ กนอ. กำหนด แต่เป็นการเสนอคุณลักษณะที่เทียบเท่าหรือดีกว่า ผู้ยื่นข้อเสนอต้องจัดทำเอกสารเปรียบเทียบคุณลักษณะดังกล่าวพร้อมแนบเอกสารมาพร้อมหนังสือรับรองด้วย

9.4 หนังสือรับรองมาตรฐาน ISO/IEC 27001:2013 สำหรับศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ (Security Operations Center: SOC ซึ่งตั้งอยู่ในประเทศไทยของผู้รับจ้าง ตามที่ระบุไว้ในข้อกำหนดและขอบเขตของงานข้อ 3.12

9.5 ข้อเสนอด้านเทคนิค เพื่อการพิจารณาด้านเกณฑ์คุณภาพตามหัวข้อการให้คะแนน **ภาคผนวก ข** ประกอบด้วย

9.5.1 ข้อเสนอด้านคุณสมบัติของผู้ยื่นข้อเสนอตามขอบเขตของงาน ข้อ 3.13 ได้แก่

(1) จำนวนงาน/โครงการที่ให้บริการศูนย์ SOC

(2) มูลค่างาน/โครงการที่ให้บริการศูนย์ SOC

(3) ระยะเวลาที่มีบริการศูนย์ SOC จนถึงปัจจุบัน (นับถึงวันยื่นข้อเสนอ)

(4) มาตรฐานศูนย์บริการ SOC

(5) ระยะเวลาในการให้บริการ SOC อย่างต่อเนื่อง

9.5.2 ข้อเสนอด้านคุณสมบัติของบุคลากรในโครงการ แต่ละตำแหน่ง

9.5.3 อธิบายหลักการทำงานของ Ransomware และแนวทางการแก้ไข

9.5.4 คุณลักษณะเฉพาะเพิ่มเติมของอุปกรณ์ 3 รายการตามขอบเขตของงาน ข้อ 4.4 ข้อ 4.9 และข้อ 4.11

(1) อุปกรณ์การเฝ้าระวังภัยคุกคามทางไซเบอร์

(2) อุปกรณ์ Endpoint Protection Platform

(3) อุปกรณ์ Web Application Firewall

ทั้งนี้ หัวข้อ 9.5.3 การอธิบายหลักการทำงานของ Ransomware และแนวทางการแก้ไข ให้จัดทำรายละเอียดแนวทางปฏิบัติโดยใช้ Endpoint Protection Platform ที่นำเสนอมาในโครงการนี้

9.6 ข้อเสนอด้านราคา

ผู้ยื่นข้อเสนอต้องเสนอราคาตามแบบและวิธีการที่กำหนดในเอกสารประกวดราคาด้วยอิเล็กทรอนิกส์ และเสนอในระบบการจัดซื้อจัดจ้างภาครัฐ (Electronic Government Procurement : e-GP) ตามวันเวลาที่กำหนด

10. เกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ในการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์โครงการจ้างบริการศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ และทดสอบความมั่นคงปลอดภัยของระบบสารสนเทศ กนอ. ประจำปี 2566-2567 ครั้งนี้ ลักษณะงานเป็นการตรวจสอบช่องโหว่ (VA) และทดสอบเจาะระบบ (Penetration Testing) ระบบสารสนเทศของ กนอ. รวมถึงให้บริการศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ (Security Operation Center : SOC) และตอบสนองต่อภัยคุกคามสำหรับเครื่องแม่ข่ายและเครื่องลูกข่ายของ กนอ. โดยจะพิจารณาโดยคำนึงถึงประสิทธิภาพต่อราคา (Price Performance) ด้วยเกณฑ์ราคาประกอบกับเกณฑ์อื่น (ข้อเสนอด้านเทคนิค) ตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 มาตรา 65 และระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ 2560 ข้อ 83 (2) ซึ่งมีสัดส่วนน้ำหนักระหว่างเกณฑ์ด้านราคาเท่ากับร้อยละ 20 และเกณฑ์อื่นๆ (ข้อเสนอด้านเทคนิค) ร้อยละ 80 โดยคณะกรรมการประกวดราคาอิเล็กทรอนิกส์จะดำเนินการเมื่อสิ้นสุดระยะเวลาการเสนอราคาในระบบอิเล็กทรอนิกส์แล้วตามลำดับ ดังนี้

10.1 จัดพิมพ์เอกสารข้อเสนอทั้งหมดของผู้ยื่นข้อเสนอทุกรายการจากระบบการประกวดราคาอิเล็กทรอนิกส์ (ยกเว้นเอกสารข้อเสนอด้านราคา) จำนวน 1 ชุด และลงลายมือชื่อกำกับไว้ทุกแผ่น

10.2 ตรวจสอบการมีผลประโยชน์ร่วมกัน และความครบถ้วนถูกต้องของเอกสารหลักฐานต่างๆ แล้วพิจารณาคัดเลือกรายที่ไม่มีผลประโยชน์ร่วมกัน มีคุณสมบัติและเอกสารหลักฐานต่างๆ ครบถ้วนถูกต้องและพิจารณาข้อเสนอด้านเทคนิคตามเกณฑ์การให้คะแนนที่กำหนดต่อไป สำหรับรายที่มีผลประโยชน์ร่วมกัน หรือมีคุณสมบัติหรือยื่นเอกสารหลักฐานต่างๆ ไม่ครบถ้วนถูกต้อง หรือไม่ครบถ้วน หรือยื่นข้อเสนอไม่ถูกต้อง คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ จะไม่พิจารณาข้อเสนอด้านเทคนิคของผู้ยื่นข้อเสนอรายนั้น เว้นแต่เป็น ข้อผิดพลาด หรือผิดหลงเพียงเล็กน้อย หรือผิดแผกไปจากเงื่อนไขของเอกสารประกวดราคาอิเล็กทรอนิกส์ในส่วนที่ มิใช่สาระสำคัญเฉพาะในกรณีที่พิจารณาเห็นว่าจะเป็นประโยชน์ต่อ กนอ. เท่านั้น

10.3 พิจารณาข้อเสนอด้านเทคนิคของผู้ยื่นข้อเสนอทุกรายที่ผ่านการพิจารณาตามข้อ 10.2 และทำการประเมินข้อเสนอด้านเทคนิคโดยมีสัดส่วนน้ำหนักรวม 80 คะแนน โดยมีคะแนนและสัดส่วนน้ำหนักในการให้คะแนนแต่ละหัวข้อ ดังนี้

10.3.1 ข้อเสนอด้านคุณสมบัติของผู้ยื่นข้อเสนอตามขอบเขตของงาน ข้อ 3.13 **(น้ำหนัก 35)**

(1) จำนวนงาน/โครงการที่ให้บริการศูนย์ SOC **(น้ำหนัก 5)**

(2) มูลค่างาน/โครงการที่ให้บริการศูนย์ SOC **(น้ำหนัก 5)**

(3) ระยะเวลาที่มีบริการศูนย์ SOC จนถึงปัจจุบัน (นับถึงวันยื่นข้อเสนอ) **(น้ำหนัก 10)**

(4) มาตรฐานศูนย์บริการ SOC **(น้ำหนัก 5)**

(5) ระยะเวลาในการให้บริการ SOC อย่างต่อเนื่อง **(น้ำหนัก 10)**

10.3.2 ข้อเสนอด้านคุณสมบัติของบุคลากรในโครงการ แต่ละตำแหน่ง **(น้ำหนัก 5)**

10.3.3 อธิบายหลักการทำงานของ Ransomware และแนวทางการแก้ไข **(น้ำหนัก 5)**

10.3.4 คุณลักษณะเฉพาะเพิ่มเติมของอุปกรณ์ 3 รายการ **(น้ำหนัก 35)**

(1) อุปกรณ์การเฝ้าระวังภัยคุกคามทางไซเบอร์ **(น้ำหนัก 15)**

(2) อุปกรณ์ Endpoint Protection Platform **(น้ำหนัก 10)**

(3) อุปกรณ์ Web Application Firewall **(น้ำหนัก 10)**

ทั้งนี้ ในการพิจารณาให้คะแนนตามหัวข้อต่างๆ ข้างต้น คณะกรรมการฯ จะพิจารณาให้คะแนนตามหลักเกณฑ์และวิธีการให้คะแนนข้อเสนอด้านเทคนิค **ภาคผนวก ข**

10.4 คณะกรรมการฯ จะนำคะแนนที่ผู้ยื่นข้อเสนอแต่ละรายได้รับตามหลักเกณฑ์และวิธีการให้คะแนนข้อเสนอด้านเทคนิค แต่ละหัวข้อแปลงเป็นน้ำหนักที่กำหนดไว้ และทำบันทึกคะแนนน้ำหนักในระบบการจัดซื้อจัดจ้างภาครัฐ (Electronic Government Procurement : e-GP) เพื่อรวมคะแนนกับเกณฑ์ราคาต่อไป โดยคะแนนข้อเสนอด้านราคาระบบ e-GP จะให้คะแนนสำหรับราคาของผู้ยื่นข้อเสนอต่ำสุด 100 คะแนน และราคาของผู้ยื่นข้อเสนอรายลำดับถัดไปจะได้คะแนนลดหลั่นตามช่วงห่างของราคา

10.5 ระบบการจัดซื้อจัดจ้างภาครัฐ (Electronic Government Procurement : e-GP) จะรวมคะแนนเกณฑ์ราคาและเกณฑ์อื่น (ข้อเสนอด้านเทคนิค) และจัดลำดับคะแนนไว้ 3 ลำดับ ผู้ยื่นข้อเสนอที่ได้รับคะแนนประเมินรวมสูงสุดจะได้รับการคัดเลือก และ กนอ. จะพิจารณาเจรจาต่อรองราคาตามที่เห็นสมควรเพื่อประโยชน์ของ กนอ. ต่อไป

10.6 กรณีผู้ได้รับการคัดเลือกไม่ไปทำสัญญาภายในวันเวลาที่กำหนด กนอ. จะพิจารณา เรียกรายลำดับถัดไปเพื่อเจรจาต่อรองและ/หรือทำสัญญาต่อไป หรืออาจพิจารณายกเลิกการประกาศเชิญชวน เพื่อดำเนินการใหม่ตามวิธีหรือขั้นตอนตามระเบียบที่เกี่ยวข้องต่อไป

11. การบอกเลิกสัญญา

11.1 ในกรณีที่ผลงานของผู้ได้รับกรคัดเลือกในขั้นตอนใดไม่ผ่านการตรวจรับจาก กนอ. และต้องปรับปรุงแก้ไขให้เป็นไปตามที่กำหนดไว้ในขอบเขตการดำเนินงานนี้หรือตามที่ได้ตกลงกัน ถ้าการแก้ไขดังกล่าวยังไม่ผ่านการตรวจรับอีก กนอ. อาจพิจารณาบอกเลิกสัญญาจ้างมิให้ดำเนินการต่อไปโดยที่ กนอ. ไม่ต้องรับผิดชอบใดๆ ทั้งสิ้น

11.2 กนอ. มีสิทธิจะบอกเลิกสัญญาจ้างในกรณีที่ กนอ. พิจารณาแล้วเห็นว่า การดำเนินงานของผู้ได้รับการคัดเลือกไม่ได้เป็นไปตามมาตรฐานวิชาชีพ หรืออาจไม่สามารถทำงานให้แล้วเสร็จตามเวลาที่กำหนดในสัญญาได้

11.3 การบอกเลิกสัญญาตามข้อ 11.1 หรือ ข้อ 11.2 กนอ. มีสิทธิริบหรือบังคับหลักประกันหรือเรียกร้องจากธนาคารผู้ออกหนังสือค้ำประกันตามสัญญาเป็นจำนวนเงินทั้งหมดหรือแต่บางส่วนก็ได้แล้วแต่ กนอ. จะเห็นสมควร ตลอดจนมีสิทธิเรียกค่าเสียหายใดๆ อันเนื่องจากผู้ได้รับการคัดเลือกไม่ปฏิบัติตามสัญญา หาก กนอ. ต้องจ้างผู้อื่นดำเนินงานโครงการนี้แทนผู้ได้รับการคัดเลือก จะต้องชดใช้ราคาที่เพิ่มขึ้นจากราคาที่กำหนดไว้ในสัญญาด้วย

11.4 กนอ. มีสิทธิบอกเลิกสัญญาก่อนกำหนดได้ โดยการบอกกล่าวล่วงหน้าอย่างน้อย 30 (สามสิบ) วัน โดยที่ กนอ.ตกลงจะจ่ายเงินค่าจ้างตามสัดส่วนของงานที่ส่งมอบและผ่านการตรวจรับแล้ว รวมทั้งเงินค่าใช้จ่ายอื่นๆ ที่เกี่ยวข้อง (ถ้ามี) ทั้งนี้การชำระเงินทั้งหมดจะต้องไม่เกินค่าจ้างตามสัญญา

12. ข้อตกลงห้ามเปิดเผยข้อมูล

ข้อมูล เอกสาร หรือสัญญาที่เกี่ยวข้องกับโครงการนี้ทั้งหมดที่ กนอ. จัดหาให้ หรือผู้รับจ้างดำเนินการและจัดหาให้ กนอ. ถือเป็นความลับ และเป็นสมบัติของ กนอ. โดยผู้รับจ้างต้องไม่เปิดเผยข้อมูลและผลการดำเนินการให้แก่ผู้ใดยกเว้นแต่จะได้รับอนุญาตจาก กนอ. เป็นลายลักษณ์อักษร หากผู้รับจ้างละเมิดโดยมีการนำไปเผยแพร่ และเปิดเผยโดยไม่ได้รับอนุญาต กนอ. มีสิทธิ์ฟ้องร้องเรียกค่าเสียหายและดำเนินการตามกฎหมายได้

13. ความคุ้มครองเกี่ยวกับลิขสิทธิ์

ในกรณีที่บุคคลภายนอกกล่าวอ้างหรือใช้สิทธิเรียกร้องใด ๆ ว่ามีการละเมิดลิขสิทธิ์เกี่ยวกับงานจ้างตามสัญญานี้ โดย กนอ. มิได้แก้ไขดัดแปลงไปจากเดิม ผู้รับจ้างจะต้องดำเนินการทั้งปวงเพื่อให้การกล่าวอ้างหรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว เพื่อให้ กนอ. สามารถใช้งานจ้างนั้นต่อไปได้ หากผู้รับจ้างมิอาจกระทำได้และ กนอ. ต้องรับผิดชอบชดใช้ค่าเสียหายต่อบุคคลภายนอก เนื่องจากผลแห่งการละเมิดลิขสิทธิ์ดังกล่าว ผู้รับจ้างต้องเป็นผู้ชำระค่าเสียหาย ค่าปรับและค่าใช้จ่ายอื่น ๆ รวมทั้งค่าธรรมเนียม และค่าทนายความ ทั้งนี้ กนอ. จะแจ้งผู้รับจ้างทราบเป็นลายลักษณ์อักษรในเมื่อได้มีการกล่าวอ้างหรือใช้สิทธิเรียกร้องดังกล่าว โดยไม่ชักช้า

14. เงื่อนไขอื่นๆ

ผู้รับจ้างต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ นโยบายคุ้มครองข้อมูลส่วนบุคคล และประมวลแนวทางปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ การนิคมอุตสาหกรรมแห่งประเทศไทย รวมถึงนโยบาย คำสั่งและขั้นตอนปฏิบัติอื่น ๆ ที่เกี่ยวข้อง

.....

ภาคผนวก ก

คุณสมบัติบุคลากร

ตำแหน่ง	คุณสมบัติ	จำนวน (คน)
1 หัวหน้าโครงการ	- วุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง - ได้รับใบรับรองความรู้ความสามารถอย่างใดอย่างหนึ่ง ดังนี้ ☐ ITIL V4 หรือ ITIL Foundation สูงกว่าหรือใหม่กว่า ☐ Lead Auditor ISO27001 ☐ CompTIA project+ ☐ CompTIA CySA+ - มีประสบการณ์ทำงานด้านเทคโนโลยีสารสนเทศ 5 ปี	1
2. ที่ปรึกษาด้านการเฝ้าระวังภัยคุกคามทางไซเบอร์	- วุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง - ได้รับใบรับรองความรู้ความสามารถอย่างใดอย่างหนึ่ง ดังนี้ ☐ Certified Information System Security Professional (CISSP) ☐ Secure Infrastructure Expert (CSIE) ☐ Certified Information Security Manager (CISM) ☐ GIAC Security Operation Manager (GSOM) ☐ GIAC Strategic Planning, Policy, and Leadership (GSTRT) - มีประสบการณ์ทำงานด้านเทคโนโลยีสารสนเทศ 5 ปี	1

ตำแหน่ง	คุณสมบัติ	จำนวน (คน)
3. หัวหน้าประจำศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ (Head of SOC)	- วุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง - ได้รับใบรับรองความรู้ความสามารถอย่างใดอย่างหนึ่ง ดังนี้ ☐ Certified Ethical Hacker (CEH) ☐ CompTIA Advanced Security Practitioner (CASP+) - มีประสบการณ์ทำงานด้านเทคโนโลยีสารสนเทศ 3 ปี	1
4 ผู้เชี่ยวชาญด้านการทดสอบเจาะระบบ	- วุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง - ได้รับใบรับรองความรู้ความสามารถอย่างใดอย่างหนึ่ง ดังนี้ ☐ Offensive Security Certified Professional (OSCP) ☐ GIAC Penetration Tester (GPEN) ☐ CompTIA Pentest+ - มีประสบการณ์ทำงานด้านเทคโนโลยีสารสนเทศ 3 ปี	1
5. ผู้ปฏิบัติงานด้านการทดสอบเจาะระบบ	- วุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง - ได้รับใบรับรองความรู้ความสามารถอย่างใดอย่างหนึ่ง ดังนี้ ☐ Certified Ethical Hacker (CEH) ☐ CompTIA Pentest+ ☐ CompTIA CASP หรือ CompTIA CASP+ - มีประสบการณ์ทำงานด้านเทคโนโลยีสารสนเทศ 2 ปี	1

ตำแหน่ง	คุณสมบัติ	จำนวน (คน)
6. เจ้าหน้าที่ปฏิบัติการและวิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Analyst) ระดับ 3	- วุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง - ต้องได้รับใบรับรองความรู้ความสามารถอย่างใดอย่างหนึ่งดังนี้ ☐ CompTIA CASP+ หรือ CASP หรือ CySA+ ☐ Certified Ethical Hacker (CEH) - มีประสบการณ์ทำงานด้านเทคโนโลยีสารสนเทศ 3 ปี	1
7. เจ้าหน้าที่ปฏิบัติการและวิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Analyst) ระดับ 2	- วุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง - ได้รับใบรับรองความรู้ความสามารถอย่างใดอย่างหนึ่งดังนี้ ☐ CompTIA CySA+ ☐ CompTIA Security+ - มีประสบการณ์ทำงานด้านเทคโนโลยีสารสนเทศ 2 ปี	1
8. เจ้าหน้าที่ปฏิบัติการและวิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Analyst) ระดับ 1	- วุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง - ได้รับใบรับรองความรู้ความสามารถอย่างใดอย่างหนึ่งดังนี้ ☐ CompTIA Security+ ☐ CompTIA CySA+ - มีประสบการณ์ทำงานด้านเทคโนโลยีสารสนเทศ 1 ปี	4

ภาคผนวก ข

หลักเกณฑ์และวิธีการให้คะแนน รายละเอียดการนำเสนอทางเทคนิค

ลำดับ	หัวข้อการพิจารณาให้คะแนน	คะแนน
1.	**คุณสมบัติของผู้ยื่นข้อเสนอตามขอบเขตของงาน ข้อ 3.13 (น้ำหนัก 35)** ผู้ยื่นข้อเสนอต้องมีศูนย์บริการเฝ้าระวังด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Operation Center : SOC) โดยให้บริการตลอด 24 ชั่วโมงต่อวัน 7 วันต่อสัปดาห์ (24x7) และให้บริการอยู่ในปัจจุบัน ซึ่งเป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐ หรือหน่วยงานเอกชนที่ กนอ. เชื่อถือ ทั้งนี้ผู้ยื่นข้อเสนอต้องแสดงหนังสือรับรองผลงานหรือสำเนาสัญญาฯ หรือเอกสารยืนยันการจ้างพร้อมกับการยื่นข้อเสนอด้วย	
	1.1 จำนวนงาน/โครงการที่ให้บริการศูนย์บริการเฝ้าระวังด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Operation Center : SOC) อยู่ในปัจจุบัน **คะแนนเต็ม 100 คะแนน (น้ำหนัก 5)**	
	(1) จำนวน 1 งาน/โครงการ	60
	(2) จำนวน 2 งาน/โครงการ	70
	(3) จำนวน 4 งาน/โครงการ	80
	(4) จำนวน 8 งาน/โครงการ	90
	(5) จำนวนมากกว่า 10 งาน/โครงการ	100
	1.2 มูลค่าของงาน/โครงการที่ให้บริการศูนย์บริการเฝ้าระวังด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Operation Center : SOC) อยู่ในปัจจุบัน (พิจารณาเฉพาะมูลค่าของงาน/โครงการที่มากที่สุด **คะแนนเต็ม 100 คะแนน (น้ำหนัก 5)**	
	(1) มูลค่าไม่เกิน 2,000,000 บาท	50
	(2) มูลค่ามากกว่า 2,000,000 บาท แต่ไม่เกิน 6,000,000 บาท	60
	(3) มูลค่ามากกว่า 6,000,000 บาท แต่ไม่เกิน 10,000,000 บาท	70
	(4) มูลค่ามากกว่า 10,000,000 บาท แต่ไม่เกิน 14,000,000 บาท	80
	(5) มูลค่ามากกว่า 14,000,000 บาท แต่ไม่เกิน 20,000,000 บาท	90
	(6) มูลค่ามากกว่า 20,000,000 บาท	100
	1.3 ระยะเวลาที่ให้บริการศูนย์บริการเฝ้าระวังด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Operation Center : SOC) จนถึงปัจจุบัน (พิจารณาระยะเวลานับแต่เปิดบริการและมีบริการต่อเนื่องถึงปัจจุบัน (นับถึงวันที่ยื่นข้อเสนอ) **คะแนนเต็ม 100 คะแนน (น้ำหนัก 10)**	

ลำดับ	หัวข้อการพิจารณาให้คะแนน	คะแนน
	(1) ไม่เกิน 2 ปี	60
	(2) มากกว่า 2 ปี แต่ไม่เกิน 5 ปี	70
	(3) มากกว่า 5 ปี แต่ไม่เกิน 8 ปี	80
	(4) มากกว่า 8 ปี แต่ไม่เกิน 10 ปี	90
	(5) มากกว่า 10 ปี	100
	1.4 มาตรฐานศูนย์บริการเฝ้าระวังด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Operation Center : SOC) (พิจารณาเฉพาะมาตรฐานที่ได้รับการรับรองแล้ว คะแนนเต็ม 100 คะแนน (น้ำหนัก 5)	
	(1) มาตรฐาน ISO 27001:2013 หรือ Version ล่าสุด	80
	(2) มาตรฐาน ISO 27001:2013 หรือ Version ล่าสุด และ NIST NSF หรือ ISO 27701:2019	90
	(3) มาตรฐาน ISO 27001:2013 หรือ Version ล่าสุด และ ISO 20000:2018	100
	1.5 ระยะเวลาในการให้บริการเฝ้าระวังด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Operation Center : SOC) อย่างต่อเนื่องของผลงานอย่างน้อย 1 โครงการ คะแนนเต็ม 100 คะแนน (น้ำหนัก 10)	
	(1) ให้บริการต่อเนื่องเป็นระยะเวลามากกว่า 1 ปี	80
	(2) ให้บริการต่อเนื่องเป็นระยะเวลามากกว่า 4 ปี	90
	(3) ให้บริการต่อเนื่องเป็นระยะเวลามากกว่า 8 ปี	100
2.	**คุณสมบัติของบุคลากรในโครงการ (คะแนนเต็ม 100 น้ำหนัก 5)** พิจารณาจากเอกสารหลักฐานเอกสารคุณสมบัติของข้อเสนอบุคลากรในโครงการตามขอบเขตของงาน ข้อ 4.13 รวม 3 ด้าน ได้แก่ (1) ด้านใบรับรองความรู้ความสามารถตามกำหนดแต่ละตำแหน่ง และ (2) ด้านประสบการณ์ โดยพิจารณาให้คะแนนเป็นรายบุคคล (กรณีในตำแหน่งใดเสนอมากกว่า 1 คน จะพิจารณาให้คะแนนเฉพาะคนที่มีคุณสมบัติดีที่สุดของตำแหน่งนั้น) ทั้งนี้ในด้านใบรับรองความรู้ความสามารถในกรณีที่เสนอสูงกว่ามาตรฐานที่กำหนดในข้อกำหนดคุณสมบัติบุคลากรให้ระบุในเอกสารที่ยื่นด้วย	
	(1) ผู้จัดการ/หัวหน้าโครงการ	20
	(2) ที่ปรึกษาด้านการเฝ้าระวังภัยคุกคามทางไซเบอร์	10
	(3) หัวหน้าประจำศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ (Head of SOC)	10
	(4) (ผู้เชี่ยวชาญด้านการทดสอบเจาะระบบ	10

ลำดับ	หัวข้อการพิจารณาให้คะแนน	คะแนน
	(5) ผู้ปฏิบัติงานด้านการทดสอบเจาะระบบ	10
	(6) เจ้าหน้าที่ปฏิบัติการและวิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Analyst) ระดับ 3	10
	(7) เจ้าหน้าที่ปฏิบัติการและวิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Analyst) ระดับ 2	10
	(8) เจ้าหน้าที่ปฏิบัติการและวิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Analyst) ระดับ 1	20
	วิธีการให้คะแนน :	
	☐ กรณีเสนอรายละเอียดครบและตรงตามข้อกำหนดทั้ง 2 ด้าน ได้ร้อยละ 80 ของคะแนน	
	☐ กรณีเสนอรายละเอียดครบและตรงตามข้อกำหนดโดยมีคุณสมบัติด้านใดด้านหนึ่งดีกว่าหรือสูงกว่าข้อกำหนด ได้ร้อยละ 90 ของคะแนน	
	☐ กรณีเสนอรายละเอียดครบและตรงตามข้อกำหนดโดยมีคุณสมบัติดีกว่าหรือสูงกว่าข้อกำหนด 2 ด้าน ได้ร้อยละ 100 ของคะแนน	
3.	**อธิบายการทำงานของ Ransomware คะแนนเต็ม 100 คะแนน (น้ำหนัก 5)** ผู้ยื่นข้อเสนอต้องทำการสรุปการทำงานของ Ransomware และวิธีการจัดการเมื่อเกิดเหตุการณ์ Ransomware ที่ตรวจพบ รวมทั้งแสดงการเก็บหลักฐานเพื่อวิเคราะห์และดำเนินการ (forensic) ของ Ransomware Blackcat หรือ Ransomware Lockbit โดยใช้ Endpoint Protection Platform ที่นำเสนอ	
	☐ อธิบายพร้อมเอกสารประกอบและรายงานสรุปการทำงานของ Ransomware	80
	☐ อธิบายพร้อมเอกสารประกอบและรายงานสรุปการทำงานของ Ransomware ☐ อธิบายพร้อมเอกสารประกอบและรายงานสรุปการจัดการ Ransomware	90
	☐ อธิบายพร้อมเอกสารประกอบและรายงานสรุปการทำงานของ Ransomware ☐ อธิบายพร้อมเอกสารประกอบและรายงานสรุปการจัดการ Ransomware ☐ อธิบายพร้อมเอกสารประกอบและรายงานสรุปการเก็บหลักฐานเพื่อการวิเคราะห์และการดำเนินการต่อในการแก้ไขปัญหา	100
4.	**คุณลักษณะเฉพาะเพิ่มเติมของอุปกรณ์ 3 รายการ (น้ำหนักรวม 35)** รายละเอียดคุณลักษณะเฉพาะของอุปกรณ์ 3 รายการ ตามขอบเขตของงาน ข้อ 4.4 ข้อ 4.9 และข้อ 4.11 ซึ่งต้องมีคุณสมบัติตรงตามที่กำหนดในขอบเขตของงาน และจะพิจารณาให้คะแนนคุณภาพประสิทธิภาพสำหรับคุณลักษณะเฉพาะทางเทคนิคเพิ่มเติมซึ่งเป็นคุณสมบัติตามมาตรฐานของผลิตภัณฑ์ เฉพาะที่เป็นประโยชน์ต่อโครงการนี้	

ลำดับ	หัวข้อการพิจารณาให้คะแนน	คะแนน
	4.1 คุณลักษณะเฉพาะเพิ่มเติมของอุปกรณ์การเฝ้าระวังภัยคุกคามทางไซเบอร์ คะแนนเต็ม 100 คะแนน (น้ำหนัก 15)	
	(1) แสดงเหตุการณ์การโจมตีในรูปแบบแผนภาพและเห็นความเชื่อมโยงของการโจมตีในรูปแบบของ Attack Tree	8
	(2) ความสามารถตรวจจับและตอบสนองภัยคุกคามทางไซเบอร์ในระดับเครือข่าย (Network Detection and Response)	18
	(3) ความสามารถในการระบบวิเคราะห์ไฟล์ต้องสงสัย (Malware Sandbox)	10
	(4) มีฐานข้อมูลอัจฉริยะ (Threat Intelligence)	4
	(5) ความสามารถวิเคราะห์พฤติกรรมผู้ใช้ (Users and Entity Behavior Analytics)	8
	(6) ความสามารถในการตอบสนองภัยคุกคามอัตโนมัติ (Security orchestration, Automation and Response)	22
	(7) ความสามารถในการติดตามการเปลี่ยนแปลงไฟล์ (File Integrity Monitoring) เช่น การเปลี่ยนแปลงไฟล์ Create, Delete, และ Change ได้เป็นอย่างน้อย	18
	(8) ความสามารถวิเคราะห์ภัยคุกคามทางไซเบอร์ โดยใช้ Machine Learning ทั้งในรูปแบบของ Unsupervised ML และ Supervised ML และ เข้ามาช่วยรวบรวม Alert ที่มีความสัมพันธ์กันมาจัดกลุ่มรวมกัน (Correlation) และนำเสนอกลุ่มของ Alert ให้อยู่ในรูปของแบบ ของ Graph หรือ Diagram ที่แสดงรายละเอียดการโจมตีหรือพฤติกรรมต่างๆของการโจมตี	12
	วิธีการให้คะแนน :	
	☐ กรณีมีคุณลักษณะเฉพาะทางเทคนิคเพิ่มเติมตามข้อย่อยหนึ่งข้อย่อยใด ก็จะได้คะแนนในแต่ละหัวข้อย่อยนั้น ๆ ☐ กรณีไม่มีคุณลักษณะเฉพาะทางเทคนิคเพิ่มเติม ก็จะไม่ได้คะแนนในหัวข้อนี้	
	4.2 คุณลักษณะเฉพาะเพิ่มเติมของอุปกรณ์ Endpoint Protection Platform คะแนนเต็ม 100 คะแนน (น้ำหนัก 10)	
	(1) ระบบสามารถแสดงรายการ Application ผ่านหน้าบริหารการจัดการ เพื่อตรวจสอบว่ามี Application อะไรบ้างที่ติดตั้งบนเครื่องคอมพิวเตอร์ปลายทาง รวมถึงตรวจสอบช่องโหว่บน Application โดยสามารถรองรับ MITRE CVE database ได้ และสามารถทำงานได้บนระบบปฏิบัติการทั้ง Windows, macOS และ Linux ได้เป็นอย่างน้อย	8

ลำดับ	หัวข้อการพิจารณาให้คะแนน	คะแนน
	(2) ความสามารถรองรับการควบคุมอุปกรณ์ Bluetooth & BLE โดยกำหนด Rule หรือ Policy สามารถระบุ Bluetooth Version หรือ Hardware identifier ที่จะอนุญาต (Allow) หรือ ไม่อนุญาต (Block) ให้ใช้งานบนเครื่องคอมพิวเตอร์ปลายทางได้	8
	(3) ความสามารถทำงานร่วมกับ Active Directory, Syslog ด้วย format CEF หรือ CEF2, Threat Intelligence เช่น VirusTotal, Recorded Future เป็นต้น, Email และรองรับ API กับโซลูชั่นอื่น ๆ เพื่อรับมือกับภัยคุกคาม	8
	(4) ความสามารถในการตรวจจับและป้องกันภัยคุกคามได้แม้เครื่องคอมพิวเตอร์ปลายทางขาดการเชื่อมต่อ (Offline) รวมถึงไม่จำเป็นต้อง Update ฐานข้อมูลไวรัสจากเครื่องคอมพิวเตอร์ปลายทาง	8
	(5) ความสามารถสแกนควบคุมการใช้งานอุปกรณ์ Removable Media หรือ Network Drive ได้ และสามารถควบคุมการใช้งานอุปกรณ์ต่อพ่วง (Endpoint Control หรือ Peripheral Control หรือ Device Control) ผ่าน USB โดยกำหนดให้สามารถ Read & Write, Read Only หรือ Block สำหรับเครื่องคอมพิวเตอร์ปลายทาง รวมถึงสามารถระบุ Vendor, Vendor ID, Serial ID, Product ID หรือ Class หรือ Model ที่อนุญาตให้ใช้งานบนเครื่องคอมพิวเตอร์ปลายทางได้	8
	(6) ความสามารถแสดงรายการ Application ผ่านหน้าบริหารการจัดการ เพื่อตรวจสอบว่ามี Application อะไรบ้างที่ติดตั้งบนเครื่องคอมพิวเตอร์ปลายทาง รวมถึงตรวจสอบช่องโหว่บน Application โดยรองรับ MITRE CVE Database ได้	12
	(7) ความสามารถทำการเก็บหลักฐานการโจมตีที่เกิดขึ้นบนเครื่องคอมพิวเตอร์ปลายทางเพื่อตรวจสอบย้อนหลังได้ไม่น้อยกว่า 14 วัน สำหรับค่าต่างๆ ในการค้นหา เช่น Hostname, OS, Domain Name, IP address, Hash, MD5, SHA1 และ Process ได้เป็นอย่างน้อยและรองรับการขยายการเก็บข้อมูลได้ไม่น้อยกว่า 1 ปี	24
	(8) ความสามารถทำการกู้คืนระบบ (Rollback) ของคอมพิวเตอร์ปลายทาง เมื่อถูกโจมตีจาก Ransomware หรือ Malicious และรองรับการกู้คืนระบบแบบอัตโนมัติ ผ่านหน้าบริหารการจัดการ โดยไม่จำเป็นต้องเขียน Script เพื่อใช้ในการกู้คืน หรือสามารถนำเสนอระบบกู้คืนข้อมูลเพิ่มเติมได้	24
	วิธีการให้คะแนน :	
	☐ กรณีมีคุณลักษณะเฉพาะทางเทคนิคเพิ่มเติมตามข้อย่อยหนึ่งข้อย่อยใด ก็จะได้คะแนนในแต่ละหัวข้อย่อยนั้น ๆ ☐ กรณีไม่มีคุณลักษณะเฉพาะทางเทคนิคเพิ่มเติม ก็จะไม่ได้คะแนนในหัวข้อนี้	

ลำดับ	หัวข้อการพิจารณาให้คะแนน	คะแนน
	4.3 คุณลักษณะเฉพาะเพิ่มเติมของอุปกรณ์ Web Application Firewall **คะแนนเต็ม 100 คะแนน (น้ำหนัก 10)**	
	(1) ระบบ Web Application Firewall ที่นำเสนอใช้งาน Sub-Domain ได้มากกว่า 9 sub-domain	20
	(2) ระบบ Web Application Firewall ที่นำเสนอมีเครือข่ายที่สามารถป้องกัน DDoS ได้มากกว่า 110 Tbps	20
	(3) ระบบ Web Application Firewall ที่นำเสนอต้องสามารถป้องกันการโจมตีในระดับเครือข่าย (DDoS Attack) แบบไม่จำกัดจำนวนครั้ง และขนาดของการโจมตี	2.5
	(4) สามารถทำการวิเคราะห์และแยกแยะบอทและมนุษย์โดยใช้เทคนิค Heuristics, Machine Learning (ML) และ JavaScript Detections (JSD) ได้เป็นอย่างน้อย	2.5
	(5) สามารถตั้งค่า Web Application Firewall (WAF) และสามารถแก้ไข เพิ่ม Custom WAF Rules ได้ไม่น้อยกว่า 1000 rules	2.5
	(6) ให้บริการป้องกันการโจมตีในระดับเครือข่าย (DDoS Attack) แบบไม่จำกัดจำนวนครั้ง และขนาดของการโจมตี โดยไม่มีค่าใช้จ่ายเพิ่มเติม	20
	(7) บริการที่เสนอรองรับการส่ง Raw Log ผ่านทาง Log Push ไปยัง Amazon S3, Azure Blob Storage, Google Cloud Storage, or Sumo Logic ได้เป็นอย่างน้อย และ Log Pull REST API	2.5
	(8) สามารถลดขนาด บีบอัด และทำการลบ Metadata ของไฟล์ โดย สามาถเลือกได้ทั้งแบบ Lossless และ Lossy รวมถึงรองรับ WebP	10
	(9) สามารถแสดงรายงาน (Analytic) บน Dashboard แบบ Real-time หรือ Near Real-time โดย Dashboard ที่แสดงต้องประกอบด้วยข้อมูล Total Requests, Cached Request, Bandwidth Saved, Threat Sources, Top Threat Origin และTop Traffic Origin ได้เป็นอย่างน้อย	10
	(10) ระบบ Web Application Firewallที่นำเสนอมี Data Center หรือ Point of Presence (PoP) อย่างน้อย 220 จุดทั่วโลก และ PoP อย่างน้อย 6 จุดในไทย	10
	วิธีการให้คะแนน : ☐ กรณีมีคุณลักษณะเฉพาะทางเทคนิคเพิ่มเติมตามข้อย่อยหนึ่งข้อย่อยใด ก็จะได้คะแนนในแต่ละหัวข้อย่อยนั้น ๆ ☐ กรณีไม่มีคุณลักษณะเฉพาะทางเทคนิคเพิ่มเติม ก็จะไม่ได้คะแนนในหัวข้อนี้	