ขอบเขตของงานและคุณลักษณะเฉพาะ
ซื้อระบบตรวจจับและตอบสนองภัยคุกคามบนอุปกรณ์ปลายทาง
(Endpoint Detection and Response: EDR) พร้อมลิขสิทธิ์การใช้งาน ๒ ปี

๑. ความเป็นมา

ปัจจุบันสถาบันพระบรมราชชนกมีการใช้ระบบเทคโนโลยีสารสนเทศและอุปกรณ์ปลายทาง (Endpoint) เช่น เครื่องคอมพิวเตอร์แม่ข่าย (Server) เครื่องคอมพิวเตอร์ลูกข่าย (Client) และอุปกรณ์พกพา เพื่อสนับสนุนภารกิจด้านการบริหารจัดการ การเรียนการสอน การวิจัย รวมถึงการให้บริการด้านสาธารณสุขและการแพทย์ ซึ่งระบบสารสนเทศดังกล่าวมีความสำคัญและเกี่ยวข้องกับข้อมูลที่มีความอ่อนไหวและข้อมูลส่วนบุคคลจำนวนมากอย่างไรก็ตาม สถานการณ์ด้านภัยคุกคามทางไซเบอร์ในปัจจุบันมีแนวโน้มทวีความรุนแรงและซับซ้อนมากขึ้น อาทิ การโจมตีด้วยมัลแวร์ขั้นสูง (Advanced Malware) การโจมตีแบบแรนซัมแวร์ (Ransomware) การลักลอบเข้าถึงระบบโดยไม่ได้รับอนุญาต รวมถึงการโจมตีที่อาศัยช่องโหว่ของอุปกรณ์ปลายทาง ซึ่งระบบป้องกันแบบเดิม เช่น โปรแกรมป้องกันไวรัสทั่วไป อาจไม่สามารถตรวจจับหรือรับมือกับภัยคุกคามรูปแบบใหม่ได้อย่างมีประสิทธิภาพเพื่อยกระดับความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันพระบรมราชชนก ให้สอดคล้องกับแนวทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่ดีมาตรฐานสากลด้านความปลอดภัยสารสนเทศ เช่น ISO/IEC ๒๗๐๐๑ รวมถึงนโยบายและแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ของภาครัฐ จึงมีความจำเป็นต้องจัดหาระบบตรวจจับและตอบสนองภัยคุกคามบนอุปกรณ์ปลายทาง (Endpoint Detection and Response: EDR) เพื่อใช้ในการเฝ้าระวังตรวจจับ วิเคราะห์ และตอบสนองต่อเหตุการณ์ด้านความปลอดภัยได้อย่างทันท่วงที ลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อระบบสารสนเทศและภารกิจหลักของหน่วยงาน

สถาบันพระบรมราชชนก กองเทคโนโลยีดิจิทัล ได้จัดทำโครงการบริหารจัดการองค์กรและพัฒนาระบบสารสนเทศเพื่อสนับสนุนการดำเนินงานตามนโยบายและพันธกิจของสถาบัน โดยมุ่งเน้นการยกระดับความมั่นคงปลอดภัยไซเบอร์ด้วยการใช้ระบบตรวจจับและเทคโนโลยีปัญญาประดิษฐ์ (AI) ป้องกันภัยคุกคามที่มีแนวโน้มเพิ่มขึ้นในสถาบันการศึกษาและปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงการคุ้มครองข้อมูลส่วนบุคคลของนักศึกษา อาจารย์ และบุคลากรตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โครงการนี้ครอบคลุมการจัดหาครุภัณฑ์คอมพิวเตอร์และการพัฒนาโครงสร้างพื้นฐานดิจิทัลของสถาบันฯ เพื่อให้มีประสิทธิภาพรองรับการบริหารจัดการและการจัดการเรียนการสอนตามพันธกิจของสถาบันพระบรมราชชนก

๒. วัตถุประสงค์

๑. เพื่อยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันฯ ด้วยการใช้ระบบตรวจจับและเทคโนโลยีปัญญาประดิษฐ์ (AI)

๒. เพื่อยกระดับความตระหนัก ความรอบรู้ และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ของผู้บริหารและบุคลากร เพื่อป้องกันความเสี่ยงจากภัยคุกคามไซเบอร์

๓. เพื่อพัฒนาระบบและกลไกการบริหารจัดการความปลอดภัยไซเบอร์ให้มีความทันสมัย สอดคล้องกับมาตรฐานสากลและข้อกำหนดของภาครัฐ

๓. คุณสมบัติของผู้ยื่นข้อเสนอ

๑. มีความสามารถตามกฎหมาย
๒. ไม่เป็นบุคคลล้มละลาย
๓. ไม่อยู่ระหว่างเลิกกิจการ

๔. ไม่เป็นบุคคล...

๔. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๕. ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๖. มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๗. เป็นนิติบุคคล ผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๘. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอราคารายอื่นที่เข้ายื่นข้อเสนอให้แก่สถาบันพระบรมราชชนก ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม ในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๙. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

๑๐. ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงาน สิ่งของหรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

๑๑. ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) ของกรมบัญชีกลาง

๑๒. ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ เป็นไปตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ด่วนที่สุด ที่ กค (กวจ) ๐๔๐๕.๒/ว ๑๒๔ ลงวันที่ ๑ มีนาคม ๒๕๖๖ ดังนี้

มูลค่าสุทธิของกิจการ

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงว่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า ๑ ล้านบาท

(๓) สำหรับ...

(๓) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา โดยพิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคาร เป็นมูลค่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ที่ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

(๔) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในครั้งนั้น (สินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคาร

(๕) กรณีตามข้อ (๑) – (๔) ไม่ใช้บังคับกับกรณีดังต่อไปนี้

(๕.๑) กรณีผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(๕.๒) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการ ตามพระราชบัญญัติล้มละลาย (ฉบับที่ ๑๐) พ.ศ. ๒๕๖๑

๔. รายละเอียดคุณลักษณะเฉพาะของพัสดุ

ผู้ยื่นข้อเสนอต้องดำเนินการจัดหา ติดตั้ง และให้บริการระบบตรวจจับและตอบสนองภัยคุกคามบนอุปกรณ์ปลายทาง (Endpoint Detection and Response: EDR) ให้สามารถใช้งานได้อย่างมีประสิทธิภาพครอบคลุมอุปกรณ์ของสถาบันพระบรมราชชนก โดยมีคุณสมบัติของระบบ และมีขอบเขตการดำเนินงานอย่างน้อยดังต่อไปนี้

๔.๑ คุณสมบัติของระบบ

ผู้ยื่นข้อเสนอต้องเสนอสิทธิการเข้าใช้งานโปรแกรม Endpoint Protection Platform สำหรับ Clients จำนวน ๓๕๐ Licenses ระยะเวลา ๒ ปี มีคุณสมบัติอย่างน้อยดังนี้

๑) สามารถวิเคราะห์ตรวจจับภัยคุกคามโดยใช้เทคโนโลยี AI/ML ในการวิเคราะห์พฤติกรรมที่เกิดขึ้นโดยใช้ข้อมูลที่ได้มาจากเครื่อง Endpoint

๒) มีซอฟต์แวร์ Agent ที่สามารถติดตั้งได้บน Platform ได้แก่ Windows, Linux, MacOS

๓) โปรแกรมที่นำเสนอต้องสามารถทำการยืนยันตัวตนกับ ระบบ ๒ Factor Authentication ได้

๔) ซอฟต์แวร์ Agent ที่นำเสนอต้องสามารถป้องกันการโจมตีที่ช่องโหว่ของระบบ (Exploit Prevention) ซึ่งรองรับ Platform Windows, Linux และ MacOS

๕) ซอฟต์แวร์ที่นำเสนอต้องสามารถป้องกันการ Exploit ไปยังช่องโหว่ (Vulnerability) เพื่อยึดเครื่อง (Compromised) ได้อย่างน้อยดังนี้

๕.๑ Address Space Layout Randomization

๕.๒ Data Execution Protection

๕.๓ Null Page Allocation

๕.๔ Heap Spray Pre-allocation

๕.๕ SEH Overwrite Protection

๖) ซอฟต์แวร์ Agent ที่นำเสนอต้องสามารถป้องกันมัลแวร์ หรือไวรัส (Malware Prevention หรือ Antivirus)

๗) ซอฟต์แวร์...

๗) ซอฟต์แวร์ Agent ที่นำเสนอต้องสามารถป้องกันการโจมตีของมัลแวร์ระดับสูง ที่ใช้เทคนิคโจมตีแบบไม่ใช้ไฟล์ (Fileless Attacks)

๘) ซอฟต์แวร์ Agent ที่นำเสนอต้องสามารถป้องกันการโจมตีโดยใช้การวิเคราะห์พฤติกรรม (indicators of attack)

๙) ซอฟต์แวร์ Agent ที่นำเสนอต้องสามารถป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware Protection)

๑๐) ซอฟต์แวร์ Agent ที่ติดตั้งบนเครื่อง Computer จะต้องมีความสามารถในการเก็บข้อมูลเพื่อใช้ในการวิเคราะห์ สำหรับเหตุการณ์แต่ละเหตุการณ์ได้อย่างน้อยดังนี้

๑๐.๑ Host info

๑๐.๒ External network connections

๑๐.๓ Detection history

๑๐.๔ User Logon Activities

๑๐.๕ Command History

๑๐.๖ Process Executions

๑๑) สามารถแสดงข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยมีรายละเอียดอย่างน้อยดังนี้

๑๑.๑ ระบุระดับความรุนแรง (Severity)

๑๑.๒ รายละเอียดเหตุการณ์และพฤติกรรม

๑๑.๓ สามารถแสดงเทคนิคของภัยคุกคามที่ตรวจพบ โดยเทียบเคียงกับ MITRE ATT&CK stage ต่าง ๆ

๑๑.๔ แสดงลำดับเหตุการณ์ที่เกิดขึ้น (Timeline)

๑๒) มีวิธีการในการตอบสนองต่อภัยคุกคาม (Response) อย่างน้อยดังนี้

๑๒.๑ แยกหรือตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ลูกข่าย (Isolate Endpoint) ได้หรือนำเสนออุปกรณ์อื่นเพิ่มเติม

๑๒.๒ สามารถสั่งการดำเนินการด้วย zsh, Powershell และ System command หรือรูปแบบอื่น ๆ ที่ดีกว่าจาก Management Console ได้ เช่น

๑) List running processes and kill processes

๒) Show network connections

๓) Navigate the file system, get or delete files, Upload files

๔) Remotely restart or shut down a host

๑๒.๓ เพิ่มค่า Hash ของไฟล์ที่ต้องการป้องกันได้ (Add to Block List)

๑๓) สามารถเพิ่ม Behavior indicators of compromise (BIOC) หรือ custom IOA เพื่อตรวจจับพฤติกรรมที่ผิดปกติ (Malicious behaviors) เพื่อให้สามารถสร้าง Alert จากเหตุการณ์ที่เคยเกิดขึ้น โดยสามารถระบุ Process Creation, File Creation, Network Connection (IPv๔, IPv๖) และ Domain Name

๑๔) ต้องมี Password หรือ token สำหรับถอดการติดตั้ง Agent จาก Management Console เพื่อป้องกันไม่ให้ User ถอนการติดตั้ง Agent software ได้

๑๕) มีความสามารถในการแจ้งเตือน (Alert) ผ่าน Email เป็นอย่างน้อย และสามารถเชื่อมต่อกับระบบภายนอก เช่น slack, pagerduty และ webhook ได้

๑๖) สามารถ...

๑๖) สามารถค้นหาข้อมูลการใช้งานภายในที่เกี่ยวข้อง (Host Search) ได้อย่างน้อยดังนี้

๑๖.๑ Host info

๑๖.๒ External network connections

๑๖.๓ Detection history

๑๖.๔ User Logon Activities

๑๖.๕ Unique Executables Written

๑๖.๖ Unique Injected Threads

๑๖.๗ Unique DLL Injections

๑๖.๘ Java injected Threads

๑๖.๙ Command History

๑๗) สามารถค้นหาข้อมูลการใช้งาน Hash (Hash Search) ได้อย่างน้อยดังนี้

๑๗.๑ PE file info

๑๗.๒ Detect History

๑๗.๓ Unresolved Detects

๑๗.๔ Process Executions

๑๘) สามารถค้นหาข้อมูลการใช้งาน Username (User Search) ได้อย่างน้อยดังนี้

๑๘.๑ User Logon Activities

๑๘.๒ Detect History

๑๘.๓ Unresolved Detects

๑๘.๔ Process Executions

๑๘.๕ Admin tool usage

๑๙) สามารถรับข้อมูลจากอุปกรณ์อื่นได้ผ่าน protocol syslog โดยสามารถรองรับในปริมาณข้อมูลอย่างน้อย ๑๐ GB ต่อวัน เป็นอย่างน้อย

๒๐) โปรแกรมที่นำเสนอต้องเป็นผลิตภัณฑ์ที่อยู่ในกลุ่ม Leader Gartner Magic Quadrant ด้าน Endpoint Protection Platforms ปี ๒๐๒๕ และ ต้องเป็นผลิตภัณฑ์ที่อยู่ในกลุ่ม Leader The Forrester Wave ด้าน Threat Intelligence Services ปี ๒๐๒๓ เพื่อให้มั่นใจว่าโปรแกรมที่เสนอเป็นโปรแกรมป้องกันภัยคุกคามที่มีประสิทธิภาพ

๒๑) โปรแกรมที่เสนอต้องได้รับการ ทดสอบจาก THE MITRE ATT&CK EVALUATIONS: ENTERPRISE ๒๐๒๕ โดยสามารถ ตรวจจับและป้องกัน (detection, protect) ได้ ๑๐๐%

๒๒) โปรแกรมที่นำเสนอต้องสามารถกำหนด policy จาก USB device class ได้อย่างน้อยดังนี้

๒๒.๑ Audio/Video

๒๒.๒ Imaging

๒๒.๓ Mass Storage

๒๒.๔ Printer

๒๓) โปรแกรมที่...

๒๓) โปรแกรมที่นำเสนอต้องสามารถกำหนดระดับการเข้าถึง (level of access) ของ USB device ได้อย่างน้อยดังนี้

๒๓.๑ Full access (or read, write and execute สำหรับ Mass storage class)

๒๓.๒ Full block

๒๓.๓ Read and write only (สำหรับ Mass storage class)

๒๓.๔ Read only (สำหรับ Mass storage class)

๒๔) โปรแกรมที่นำเสนอต้องมีบริการในการค้นหาภัยคุกคามเชิงรุก (Threat Hunting service) มาด้วย โดยผู้เชี่ยวชาญ (Human Analysis) แบบ ๒๔/๗ ครอบคลุมทุกเครื่องคอมพิวเตอร์ที่ติดตั้ง Agent เพื่อให้สามารถรับมือภัยคุกคามจากทั่วโลกได้อย่างแม่นยำและมีประสิทธิภาพ

๒๕) สามารถทำการแจ้งเตือน Incident ที่ผู้เชี่ยวชาญทำ Threat hunting โดยทำการส่ง Incident email notification ที่ตรวจพบพร้อมทั้งแนบ Direct Link ไปยัง Incident ที่เกิดขึ้น

๒๖) สามารถกำหนด Policy ตามกลุ่มของเครื่อง (Host Groups) ได้ โดยสามารถระบุกลุ่มตามเงื่อนไขได้เช่น Tag, Platform, Type, OS version, Mac address, Local/CIDR

๔.๒ ขอบเขตการดำเนินงาน

๑) ผู้ยื่นข้อเสนอต้องจัดหาระบบ Endpoint Detection and Response (EDR) ที่เป็นลิขสิทธิ์ถูกต้องตามกฎหมาย สามารถใช้งานได้ตามระยะเวลาที่กำหนด และรองรับการอัปเดตฐานข้อมูลภัยคุกคามอย่างต่อเนื่อง

๒) ระบบ EDR ต้องสามารถติดตั้งและใช้งานกับอุปกรณ์ปลายทางของสถาบันพระบรมราชชนก ได้แก่

๒.๑ เครื่องคอมพิวเตอร์แม่ข่าย (Server)

๒.๒ เครื่องคอมพิวเตอร์ลูกข่าย (Desktop / Notebook)

๒.๓ ระบบปฏิบัติการที่ใช้งานอยู่ในปัจจุบัน เช่น Windows, Linux หรือระบบปฏิบัติการอื่นตามที่สถาบันพระบรมราชชนกใช้งาน

๓) ผู้ยื่นข้อเสนอต้องดำเนินการติดตั้งและตั้งค่าระบบ EDR ให้สามารถตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามทางไซเบอร์ได้ เช่น มัลแวร์ แรนซัมแวร์ การโจมตีจากผู้ไม่หวังดี และพฤติกรรมผิดปกติของอุปกรณ์ปลายทาง

๔) ผู้ยื่นข้อเสนอต้องจัดให้มีระบบศูนย์กลางสำหรับบริหารจัดการ (Centralized Management Console) เพื่อใช้ในการเฝ้าระวัง ตรวจสอบสถานะ วิเคราะห์เหตุการณ์ และจัดทำรายงานด้านความมั่นคงปลอดภัยของอุปกรณ์ปลายทาง

๕) ผู้ยื่นข้อเสนอต้องดำเนินการกำหนดนโยบายความปลอดภัย (Security Policy) และปรับแต่งค่าการทำงานของระบบ EDR ให้เหมาะสมกับสภาพแวดล้อมและการใช้งานของสถาบันพระบรมราชชนก

๖) ผู้ยื่นข้อเสนอต้องจัดให้มีการทดสอบการทำงานของระบบ EDR หลังการติดตั้ง เพื่อยืนยันว่าระบบสามารถทำงานได้ถูกต้อง ครบถ้วน และเป็นไปตามข้อกำหนดของโครงการ

๗) ผู้ยื่นข้อเสนอต้องให้บริการถ่ายทอดความรู้ และฝึกอบรมแก่บุคลากรของสถาบันพระบรมราชชนกที่เกี่ยวข้อง เพื่อให้สามารถใช้งาน ดูแล และบริหารจัดการระบบ EDR ได้อย่างถูกต้องและมีประสิทธิภาพ

๘) ผู้ยื่นข้อเสนอต้องให้บริการบำรุงรักษา ดูแลระบบ และให้คำปรึกษาทางเทคนิคตลอดระยะเวลาการใช้งานตามสัญญา รวมถึงการสนับสนุนด้านเทคนิคเมื่อเกิดเหตุการณ์ด้านความปลอดภัยสารสนเทศ

๙) ผู้ยื่นข้อเสนอ...

๙) ผู้ยื่นข้อเสนอต้องจัดทำเอกสารประกอบโครงการ เช่น เอกสารการติดตั้ง เอกสารการตั้งค่า คู่มือการใช้งาน และรายงานผลการดำเนินงาน เพื่อส่งมอบให้แก่สถาบันพระบรมราชชนก

๔.๓ การรับประกันและการบำรุงรักษาระบบ

๑) ผู้ยื่นข้อเสนอต้องรับประกันระบบตรวจจับและตอบสนองภัยคุกคามบนอุปกรณ์ปลายทาง (Endpoint Detection and Response: EDR) รวมถึงลิขสิทธิ์การใช้งาน ระบบบริหารจัดการ และส่วนประกอบที่เกี่ยวข้อง เป็นระยะเวลาไม่น้อยกว่า ๒ ปี นับถัดจากวันที่คณะกรรมการตรวจรับพัสดุได้พิจารณาตรวจรับพัสดุเรียบร้อยแล้ว

๒) ระหว่างระยะเวลารับประกัน ผู้ยื่นข้อเสนอต้องให้บริการบำรุงรักษาระบบแบบครบวงจร (Comprehensive Maintenance) โดยไม่คิดค่าใช้จ่ายเพิ่มเติม ครอบคลุมอย่างน้อยดังต่อไปนี้

๒.๑ การอัปเดตซอฟต์แวร์ ระบบ และฐานข้อมูลภัยคุกคาม (Threat Intelligence / Signature / Engine) อย่างต่อเนื่อง

๒.๒ การแก้ไขข้อขัดข้อง (Bug Fix / Patch) และการปรับปรุงประสิทธิภาพของระบบ

๒.๓ การแก้ไขปัญหาการใช้งานที่เกิดจากความบกพร่องของระบบ EDR

๓) ผู้ยื่นข้อเสนอต้องจัดให้มีบริการสนับสนุนทางเทคนิค (Technical Support) ตลอดระยะเวลารับประกัน โดยมีช่องทางติดต่ออย่างน้อย ได้แก่ โทรศัพท์ อีเมล หรือระบบแจ้งปัญหา (Ticket System)

๔) ผู้ยื่นข้อเสนอต้องดำเนินการตอบสนองต่อการแจ้งปัญหาของสถาบันพระบรมราชชนก ตามระดับความรุนแรงของปัญหา (Service Level Agreement: SLA) อย่างน้อยดังนี้

๔.๑ กรณีระบบไม่สามารถใช้งานได้ทั้งหมดหรือเกิดเหตุการณ์ด้านความปลอดภัยร้ายแรง ต้องเริ่มดำเนินการแก้ไขภายใน ไม่เกิน ๔ ชั่วโมง

๔.๒ กรณีระบบทำงานผิดปกติบางส่วน ต้องเริ่มดำเนินการแก้ไขภายใน ไม่เกิน ๒๔ ชั่วโมง

๔.๓ กรณีปัญหาทั่วไปหรือข้อสอบถามการใช้งาน ต้องตอบกลับภายใน ไม่เกิน ๔๘ ชั่วโมง

๕) ผู้ยื่นข้อเสนอต้องให้บริการตรวจสอบและบำรุงรักษาระบบเชิงป้องกัน (Preventive Maintenance) อย่างน้อยปีละ ๒ ครั้ง เพื่อประเมินสถานะ ความพร้อมใช้งาน และประสิทธิภาพของระบบ EDR

๖) ผู้ยื่นข้อเสนอต้องให้คำปรึกษาและสนับสนุนด้านเทคนิคแก่ผู้ดูแลระบบของสถาบันพระบรมราชชนก เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมของระบบสารสนเทศ เช่น การเพิ่มหรือลดจำนวนอุปกรณ์ปลายทาง หรือการปรับปรุงโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ

๗) ผู้ยื่นข้อเสนอต้องจัดทำรายงานผลการบำรุงรักษาและการให้บริการสนับสนุนทางเทคนิค เสนอต่อสถาบันพระบรมราชชนก อย่างน้อยปีละ ๒ ครั้ง หรือเมื่อมีการร้องขอจากสถาบันพระบรมราชชนก

๕. เงื่อนไขเพิ่มเติม

๕.๑ ผู้ยื่นข้อเสนอต้องจัดทำเอกสารเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะของผู้ยื่นข้อเสนอกับรายละเอียดคุณลักษณะเฉพาะที่สถาบันพระบรมราชชนกกำหนด และให้แนบเอกสารดังกล่าวมาพร้อมกับเอกสารยื่นข้อเสนอราคาในระบบ e-GP

๕.๒ ผู้ยื่นข้อเสนอทุกรายต้องอ่านข้อความตามเอกสารฉบับนี้ ให้เข้าใจอย่างชัดแจ้ง โดยตลอดทุกประการ ไม่ว่ากรณีใด ๆ ก็ตาม ผู้ยื่นข้อเสนอจะยกข้อเรียกร้องหรือข้ออ้างโดยอาศัยเหตุที่จะละเลยไม่ปฏิบัติตามข้อความในเอกสารนี้ หรือโดยอ้างความสำคัญผิดในข้อความการจัดหา เงื่อนไข หรือข้อกำหนดแห่งเอกสารนี้มิได้

๕.๓ หากคุณสมบัติ...

๕.๓ หากคุณสมบัติของผู้ยื่นข้อเสนอข้อใดข้อหนึ่งไม่ชัดเจน สถาบันพระบรมราชชนกสงวนสิทธิ์ในการขอข้อมูลเพิ่มเติมเพื่อประกอบการพิจารณา

๕.๔ ผู้ยื่นข้อเสนอต้องศึกษาและสำรวจสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศและอุปกรณ์ปลายทางของสถาบันพระบรมราชชนก

๕.๕ ผู้ยื่นข้อเสนอต้องวิเคราะห์ความเสี่ยงและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

๕.๖ ผู้ยื่นข้อเสนอต้องจัดทำแผนการติดตั้งและดำเนินงานระบบ EDR ร่วมกับหน่วยงานที่เกี่ยวข้อง

๕.๗ ผู้ยื่นข้อเสนอต้องจัดหาระบบ EDR และลิขสิทธิ์การใช้งานที่ถูกต้องตามกฎหมาย

๕.๘ ผู้ยื่นข้อเสนอต้องเตรียมความพร้อมของระบบศูนย์กลางบริหารจัดการและโครงสร้างพื้นฐานที่เกี่ยวข้อง

๕.๙ ผู้ยื่นข้อเสนอต้องติดตั้งระบบ EDR บนอุปกรณ์ปลายทางตามแผนที่กำหนด

๕.๑๐ ผู้ยื่นข้อเสนอต้องตั้งค่าระบบ นโยบายความปลอดภัย และการแจ้งเตือนให้เหมาะสมกับการใช้งานของสถาบันพระบรมราชชนก

๕.๑๑ ผู้ยื่นข้อเสนอต้องทดสอบการทำงานของระบบ EDR ในการตรวจจับและตอบสนองต่อภัยคุกคาม

๕.๑๒ ผู้ยื่นข้อเสนอต้องแก้ไขปรับปรุงการตั้งค่าระบบตามผลการทดสอบ

๕.๑๓ ผู้ยื่นข้อเสนอต้องฝึกอบรมการใช้งานระบบ EDR แก่ผู้ดูแลระบบและบุคลากรที่เกี่ยวข้องในรูปแบบ On-Site ณ สถานที่ที่สถาบันพระบรมราชชนกจัดเตรียมให้ หรือรูปแบบออนไลน์ (Online) ตามที่สถาบันพระบรมราชชนกกำหนด โดยไม่มีค่าใช้จ่ายเพิ่มเติม

๕.๑๔ ผู้ยื่นข้อเสนอต้องถ่ายทอดองค์ความรู้ด้านการบริหารจัดการเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๕.๑๕ ผู้ยื่นข้อเสนอต้องให้บริการสนับสนุนทางเทคนิค บำรุงรักษา และปรับปรุงระบบตลอดระยะเวลาตามสัญญา

๕.๑๖ ผู้ยื่นข้อเสนอต้องให้คำปรึกษาและสนับสนุนเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

๖. มาตรฐานวิชาชีพ

ผู้ยื่นข้อเสนอตกลงเป็นเงื่อนไขสำคัญว่า ผู้ยื่นข้อเสนอจะต้องมีและใช้ผู้ที่มีมาตรฐานวิชาชีพ ดังต่อไปนี้

๖.๑ ต้องมีที่ปรึกษาที่มีประสบการณ์ การดูแลบำรุงรักษาการเฝ้าระวังความมั่นคงปลอดภัยระบบสารสนเทศ มีใบรับรอง Certified Information Systems Security Professional (CISSP) จาก (ISC)๒ หรือ ใบรับรอง Offensive Security Certified Professional (OSCP) หรือ ใบรับรอง GCCC: GIAC Critical Controls หรือ ใบรับรอง Certified Ethical Hacker (C|EH) จาก EC-council จำนวนไม่น้อยกว่า ๑ คน โดยแนบประวัติและประสบการณ์

๖.๒ ต้องมีวิศวกร ทำหน้าที่ประสานงานในโครงการ ที่มีวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี วิศวกรรมคอมพิวเตอร์ หรือวิศวกรรมไฟฟ้า หรือวิศวกรรมสารสนเทศและการสื่อสาร และมีประสบการณ์การทำงานอย่างน้อย ๓ ปี ผ่านการอบรม CompTIA Project+ จำนวนไม่น้อยกว่า ๑ คน โดยแนบเอกสารการรับรอง

๖.๓ ต้องมีเจ้าหน้าที่ด้านเทคนิคที่ได้รับหนังสือรับรอง (Certificate) ด้าน Network ได้รับ Certificate CCIE Service Provider certification อย่างน้อย ๑ ท่าน โดยแนบเอกสารการรับรอง

๖.๔ ต้องมีเจ้าหน้าที่ด้านเทคนิคที่ได้รับหนังสือรับรอง (Certificate) ด้าน System ได้รับ VMware Certified Professional (VCP) อย่างน้อย ๑ ท่าน โดยแนบเอกสารการรับรอง

๖.๕ ต้องมีเจ้าหน้าที่...

๖.๕ ต้องมีเจ้าหน้าที่ด้านเทคนิคที่ได้รับหนังสือรับรอง (Certificate) ด้าน Security ได้รับ Certificate Palo Alto Networks Certified Network Security Engineer (PCNSE) อย่างน้อย ๑ ท่าน โดยแนบเอกสารการรับรอง

ผู้ที่ชนะการเสนอราคา จะต้องจัดทำบัญชีแสดงจำนวนบุคลากรทั้งหมดดังกล่าวข้างต้น พร้อมกับระบุรายชื่อนำมาแสดงพร้อมหลักฐานต่อคณะกรรมการตรวจรับพัสดุ ภายในเวลา ๗ วันทำการ นับถัดจากวันลงนามสัญญา และพร้อมที่จะให้ผู้ซื้อหรือเจ้าหน้าที่ของผู้ซื้อตรวจสอบดูได้ตลอดระยะเวลาสัญญา

๗. กำหนดเวลาส่งมอบพัสดุ

๗.๑ กำหนดเวลาที่ต้องการใช้พัสดุ ภายใน ๙๐ วัน นับถัดจากวันลงนามในสัญญา โดยผู้ขายจะต้องส่งมอบดังนี้

๑) รายงานการติดตั้งระบบ

๒) เอกสารแสดงสิทธิ์การใช้งาน จำนวน ๓๕๐ สิทธิ์ ระยะเวลาสัญญา ๒ ปี นับจากส่งมอบงาน

๓) รายงานการทดสอบระบบทั้งหมดของโครงการ

๔) รายงานผลการจัดอบรมให้แก่ผู้ดูแลระบบและบุคลากรที่เกี่ยวข้อง

๕) คู่มือการใช้งานระบบ จำนวน ๕ ชุด พร้อมไฟล์อิเล็กทรอนิกส์ จำนวน ๑ ชุด

๗.๒ สถานที่ในการส่งมอบ ณ กองเทคโนโลยีดิจิทัล อาคาร ๖ ชั้น ๙ สถาบันพระบรมราชชนก กระทรวงสาธารณสุข ตำบลตลาดขวัญ อำเภอเมืองนนทบุรี จังหวัดนนทบุรี

๘. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

๘.๑ ใช้เกณฑ์ราคา

๘.๒ การพิจารณาผู้ชนะการยื่นข้อเสนอสถาบันจะพิจารณาจากราคารวม

๙. วงเงินงบประมาณ

๙.๑ เงินงบประมาณรายจ่ายจากเงินรายได้ของสถาบันพระบรมราชชนก ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ แผนงานยุทธศาสตร์ของสถาบันพระบรมราชชนก งบลงทุน เป็นเงินทั้งสิ้น ๓,๒๐๐,๐๐๐ บาท (สามล้านสองแสนบาทถ้วน)

๙.๒ ราคากลาง เป็นเงิน ๓,๒๐๐,๐๐๐ บาท (สามล้านสองแสนบาทถ้วน) โดยเป็นเกณฑ์ราคากลางและคุณลักษณะพื้นฐาน ที่ผ่านความเห็นชอบจากคณะกรรมการบริหารและการจัดหาระบบคอมพิวเตอร์ของสถาบันพระบรมราชชนก ตามหนังสือสถาบันพระบรมราชชนก กองเทคโนโลยีดิจิทัล ที่ สธ ๑๑๐๑/๑๑๓๘ ลงวันที่ ๒๔ กุมภาพันธ์ ๒๕๖๙

๑๐. งวดงานและการจ่ายเงิน

สถาบันพระบรมราชชนก จะจ่ายเงินค่าสิ่งของซึ่งได้รวมภาษีมูลค่าเพิ่ม ตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงแล้ว ให้แก่ผู้ขายเมื่อผู้ขายได้ดำเนินการส่งมอบพัสดุที่มีรายละเอียดตามข้อ ๗.๑ และเมื่อคณะกรรมการตรวจรับพัสดุได้ทำการตรวจรับพัสดุถูกต้อง ครบถ้วนตามสัญญาหรือข้อตกลงเรียบร้อยแล้ว

๑๑. อัตราค่าปรับ

กรณีส่งมอบเกินกำหนด โดยคิดค่าปรับเป็นรายวันไม่น้อยกว่าวันละ ๑๐๐ บาท หรือในอัตราร้อยละ ๐.๒๐ ของราคาพัสดุที่ยังไม่ได้ส่งมอบ

๑๒. การกำหนด...

๑๒. การกำหนดระยะเวลารับประกันความชำรุดบกพร่อง

ผู้ขายต้องรับประกันสินค้าเป็นระยะเวลาไม่น้อยกว่า ๒ ปี นับถัดจากวันที่ผู้ซื้อได้ตรวจรับพัสดุเรียบร้อยแล้ว

คณะกรรมการจัดทำร่างขอบเขตของงานและคุณลักษณะเฉพาะ

(ลงชื่อ).....ประธานกรรมการ
(นายดุลยวัฒน์ มาป้อง)
ผู้อำนวยการกองเทคโนโลยีดิจิทัล

(ลงชื่อ).....กรรมการ
(ว่าที่เรือตรียุทธชัย สุนทรวิภาต)
นักวิชาการคอมพิวเตอร์

(ลงชื่อ).....กรรมการ
(นายธชา ศรีนวลขาว)
นักวิชาการคอมพิวเตอร์