ขอบเขตของงาน (Terms of Reference: TOR)

โครงการจัดซื้อ

โปรแกรมรักษาความปลอดภัยและตอบสนองต่อภัยคุกคามบนเครื่องคอมพิวเตอร์ลูกข่าย (Client)

ตำบลบางพูด อำเภอปากเกร็ด จังหวัดนนทบุรี จำนวน ๒,๕๐๐ Licenses

และโปรแกรมรักษาความปลอดภัยและตอบสนองต่อภัยคุกคามบนเครื่องคอมพิวเตอร์แม่ข่าย (Server)

ตำบลบางพูด อำเภอปากเกร็ด จังหวัดนนทบุรี จำนวน ๒๐๐ Licenses

๑. ความเป็นมา

ด้วยมหาวิทยาลัยสุโขทัยธรรมาธิราช มีระบบโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศที่มีความซับซ้อนและครอบคลุมพื้นที่อย่างกว้างขวาง ซึ่งประกอบไปด้วยอุปกรณ์ปลายทางจำนวนมาก ที่ใช้ในการดำเนินกิจกรรมที่สำคัญต่างๆ ของมหาวิทยาลัย อาทิ การจัดการเรียนการสอน การทำวิจัย ตลอดจนการบริหารจัดการองค์กร อย่างไรก็ดี ในปัจจุบันสภาพแวดล้อมทางไซเบอร์มีความเสี่ยงเพิ่มสูงขึ้น และมีภัยคุกคามที่มีความซับซ้อนมากยิ่งขึ้น ซึ่งสิ่งเหล่านี้อาจก่อให้เกิดผลกระทบอย่างร้ายแรงต่อความปลอดภัยของข้อมูลและการดำเนินงานของมหาวิทยาลัยได้ ดังนั้นมหาวิทยาลัยจึงจำเป็นต้องยกระดับระบบรักษาความปลอดภัยสำหรับอุปกรณ์ปลายทาง เพื่อเสริมสร้างความแข็งแกร่งในการป้องกันภัยคุกคามทางไซเบอร์

๒. วัตถุประสงค์

๒.๑ เพื่อเพิ่มประสิทธิภาพในการป้องกันภัยคุกคามทางไซเบอร์และการโจมตีทางอินเทอร์เน็ตที่มุ่งเป้าไปยังอุปกรณ์ปลายทางภายในเครือข่ายของมหาวิทยาลัย

๒.๒ เพื่อยกระดับความสามารถในการตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามที่ซับซ้อนได้อย่างรวดเร็วและแม่นยำ โดยใช้เทคโนโลยีการรักษาความปลอดภัยขั้นสูง

๒.๓ เพื่อสร้างระบบการจัดการความปลอดภัยแบบรวมศูนย์สำหรับอุปกรณ์ปลายทางทั้งหมดในเครือข่ายมหาวิทยาลัย อันจะช่วยเพิ่มประสิทธิภาพในการบริหารจัดการและลดความเสี่ยงด้านความปลอดภัยทางไซเบอร์โดยรวม

๓. คุณสมบัติของผู้ยื่นข้อเสนอ

๓.๑ คุณสมบัติของผู้ยื่นข้อเสนอเป็นไปตามคณะกรรมการนโยบายฯ กำหนด (รายละเอียดระบุในเอกสารประกาศประกวดราคา/หนังสือเชิญชวน)

๓.๒ ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย โดยให้ยื่นขณะเข้าเสนอราคา

๓.๓ ผู้ขายต้องมีศูนย์เฝ้าระวังและตอบสนองภัยคุกคามทางไซเบอร์ (CSOC) ได้รับใบรับรองในการดำเนินการภายใต้มาตรฐาน ISO ๒๗๐๐๑ (Information Security Management System - ISMS)

๓.๔ ผู้ยื่นข้อเสนอต้องมีผลงานประเภทเดียวกันกับงานที่ประกวดราคา และเป็นผลงานที่มีวงเงินไม่น้อยกว่า ๓,๘๐๐,๐๐๐ บาท (สามล้านแปดแสนบาทถ้วน) โดยแนบเอกสารหนังสือรับรองผลงานมาพร้อมการยื่นเอกสารเสนอราคา

๔. รายการคอมพิวเตอร์ที่ซื้อขาย

๔.๑ โปรแกรมรักษาความปลอดภัยและตอบสนองต่อภัยคุกคามบนเครื่องคอมพิวเตอร์ลูกข่าย (Client) ตำบลบางพูด อำเภอปากเกร็ด จังหวัดนนทบุรี จำนวน ๒,๕๐๐ Licenses

๔.๒ โปรแกรมรักษาความปลอดภัยและตอบสนองต่อภัยคุกคามบนเครื่องคอมพิวเตอร์แม่ข่าย (Server) ตำบลบางพูด อำเภอปากเกร็ด จังหวัดนนทบุรี จำนวน ๒๐๐ Licenses

๕. คุณลักษณะเฉพาะของครุภัณฑ์

โครงการจัดซื้อโปรแกรมรักษาความปลอดภัยและตอบสนองต่อภัยคุกคามในครั้งนี้ ประกอบไปด้วยรายละเอียดต่าง ๆ ดังต่อไปนี้

๕.๑ โปรแกรมรักษาความปลอดภัยและตอบสนองต่อภัยคุกคามบนเครื่องคอมพิวเตอร์ลูกข่าย (Client) ตำบลบางพูด อำเภอปากเกร็ด จังหวัดนนทบุรี จำนวน ๒,๕๐๐ Licenses มีคุณสมบัติทางเทคนิคดังนี้

๕.๑.๑ สามารถป้องกัน Malware บนระบบปฏิบัติการดังต่อไปนี้ได้

๑) Windows ๑๐

๒) Windows ๑๑

๓) Mac OS

๕.๑.๒ สามารถควบคุมและบริหารจัดการโปรแกรมรักษาความปลอดภัยและตอบสนองต่อภัยคุกคามผ่านทาง Web-Based Management Console บนระบบ Software as a Service (SaaS) เพื่อกำหนดนโยบายด้านความปลอดภัย (Security Policy) และบังคับใช้นโยบายด้านความปลอดภัยดังกล่าวไปยังเครื่องคอมพิวเตอร์ลูกข่าย (Client) โดยรองรับทั้ง Endpoint, Workload และ XDR เป็นอย่างน้อย

๕.๑.๓ สามารถตรวจสอบ Malware แบบอ้างอิงจากฐานข้อมูล (Signature) และแบบวิเคราะห์พฤติกรรมอย่างน้อยดังนี้ Virtual Patching หรือ Host-based Intrusion Prevention System หรือ Exploit Prevention

๕.๑.๔ สามารถตรวจสอบ Malware ได้ด้วยเทคโนโลยีดังต่อไปนี้

๑) Behavior Monitoring

๒) Machine Learning

๓) Artificial Intelligence (AI)

๔) Ransomware Protection

๕.๑.๕ สามารถป้องกันช่องโหว่ของระบบปฏิบัติการโดยที่ไม่ต้องทำการติดตั้ง Patches บนระบบปฏิบัติการจริง (Virtual Patching) เพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการ Patches ได้ หรือทำ Exploit Protection ได้

๕.๑.๖ สามารถค้นหาและป้องกันข้อมูลสำคัญของมหาวิทยาลัยไม่ให้รั่วไหลออกไปภายนอกองค์กร (Data Loss Prevention) ผ่านทาง FTP, HTTP, email, Printer, Windows Clipboard, และ Removable Storage ได้ โดยใช้เงื่อนไขอย่างน้อยดังนี้ File Attributes, Keywords และ Regular Expressions หรือเสนอระบบอื่นเพิ่มเติมเพื่อให้ได้คุณสมบัติตามที่มหาวิทยาลัยกำหนด

๕.๑.๗ สามารถทำการป้องกันโปรแกรมประยุกต์ที่ไม่ได้รับอนุญาตให้ติดตั้งใช้งานเครื่องคอมพิวเตอร์ลูกข่ายได้ (Application Control) และสามารถกำหนด Rule โดยใช้เงื่อนไขต่างๆ เช่น Lockdown, Block และ Allow ได้ หรือเสนอระบบอื่นเพิ่มเติมเพื่อให้สามารถทำ Application Control ได้

๕.๑.๘ สามารถป้องกัน Ransomware ด้วยการตรวจพฤติกรรม

๕.๑.๙ สามารถทำการป้องกันอันตรายที่มาจากการเข้าใช้งานเว็บไซต์ต่างๆ (Web Threats) โดยใช้ Web Reputation

๕.๑.๑๐ สามารถกำหนดสิทธิ์การใช้งาน เช่น Full Access, Read, Read and Execute, Modify, List Content ให้กับอุปกรณ์ USB Storage devices ได้ และสามารถอนุญาตให้ใช้งาน USB Storage ได้เป็นรายยี่ห้อ (Vendor ID) และ Serial Number ที่มีการลงทะเบียนในโปรแกรมรักษาความปลอดภัยและตอบสนองต่อภัยคุกคามบนเครื่องคอมพิวเตอร์ลูกข่ายเท่านั้น หรือเทียบเท่า

๕.๑.๑๑ สามารถกำหนดระดับการใช้งาน CPU ของเครื่องคอมพิวเตอร์ลูกข่ายระหว่างการ scan ได้

๕.๑.๑๒ สามารถข้ามการทำงานของ Scheduled Scan ได้โดยอัตโนมัติ กรณีเครื่องคอมพิวเตอร์ลูกข่ายที่ใช้เป็นแบบ Notebook และมีระดับกระแสไฟฟ้าในแบตเตอรี่ต่ำกว่าที่กำหนด

๕.๑.๑๓ สามารถหยุดการทำงานของ Scheduled Scan ได้โดยอัตโนมัติ เมื่อใช้เวลาในการ Scan นานเกินกว่าที่กำหนด

๕.๑.๑๔ ระบบป้องกันไวรัสบนเครื่องลูกข่ายสามารถป้องการการหยุดการทำงาน และถอนการติดตั้ง (Remove or Uninstall) โดยใช้รหัสผ่านได้

๕.๑.๑๕ สามารถกำหนดนโยบายการอัพเดทให้เครื่องคอมพิวเตอร์ลูกข่ายที่ถูกกำหนดให้ทำหน้าที่แจกจ่าย Pattern ให้แก่เครื่องอื่นๆ ในมหาวิทยาลัยได้ (Update Agent)

๕.๑.๑๖ ระบบที่นำเสนอต้องสามารถตรวจจับและตอบสนองต่อภัยคุกคาม เพื่อการค้นหาและวิเคราะห์ภัยคุกคามที่มาจากแหล่งต่างๆ แบบเชิงลึก (Extended Detection and Response; XDR) ได้

๕.๑.๑๗ สามารถตอบสนองภัยคุกคามที่เกิดขึ้นแบบอัตโนมัติ (Security Playbooks) เพื่อลดภาระงานของผู้ดูแลระบบ โดยจะต้องมี Pre-defined Templates มาให้ และสามารถกำหนดตามความต้องการเพิ่มเติมได้ (Customize)

๕.๑.๑๘ สามารถกำหนดสิทธิ์ของผู้ดูแลระบบในระดับที่แตกต่างกัน และสิทธิ์ที่ต่างกันได้ (User Role) โดยทำการกำหนดผู้ใช้งานและทำการ Authentication ผ่านทาง Active Directory ของมหาวิทยาลัย

(On-premise or Microsoft Entra ID) แบบตรวจสอบและยืนยันตัวตนหลายขั้นตอนการพิสูจน์ตัวจริงด้วยปัจจัยหลายอย่าง (Multi-Factor Authentication : MFA)

๕.๑.๑๙ ผู้ดูแลระบบสามารถออกรายงานการทำงานในรูปแบบ PDF, DOCX, และ XLSX ได้

๕.๑.๒๐ มีการทำ MITRE ATT&CK mapping หรือ MITRE Tactics ของภัยคุกคามที่ตรวจพบได้

๕.๑.๒๑ สามารถส่งคำสั่งจากระบบ เช่น Isolate endpoint, remote shell, remote custom script, collect file, Dump Process Memory, Terminate Process และ add to block list เพื่อตอบสนองต่อภัยคุกคามที่พบได้

๕.๑.๒๒ สามารถเก็บบันทึกรายละเอียดกิจกรรมของเครื่องคอมพิวเตอร์ลูกข่าย ได้แก่ Domain Name, EndpointID, EndpointName, IPv๔, IPv๖, URL, Port, FileSHA, FileFullPath, ProcessFullPath, CLICommand, RegistryKey และ RegistryValue ได้เป็นอย่างน้อย

๕.๑.๒๓ สามารถทำการเก็บข้อมูลหลักฐาน การแจ้งเตือน (Alert) เพื่อใช้ในการวิเคราะห์ (investigation) ที่เกี่ยวข้องกับความปลอดภัย ย้อนหลังได้ไม่น้อยกว่า ๙๐ วัน โดยมีการเก็บข้อมูลไว้บนบริการที่ได้รับมาตรฐาน ISO ๒๗๐๐๑ เป็นอย่างน้อย

๕.๑.๒๔ สามารถแสดงการแจ้งเตือนที่สอดคล้องกับ Detection Models เพื่อทำการวิเคราะห์หาสาเหตุที่แท้จริงและผลกระทบ (Root Cause and Impact Analysis)

๕.๑.๒๕ สามารถส่งข้อมูลเกี่ยวกับการโจมตีทางไซเบอร์ในเหตุการณ์นั้นๆ (Indicator of Compromise : IoC) ไปยังอุปกรณ์เครือข่ายอื่นๆ ได้ เช่น Firewall, Web Proxy และ Malware Information Sharing Platform (MISP) เป็นต้น

๕.๑.๒๖ ผลิตภัณฑ์ที่นำเสนอต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ Endpoint Protection Platforms ปีล่าสุด และได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Forrester Wave ในกลุ่มผลิตภัณฑ์ Endpoint Security ปีล่าสุด

๕.๒ โปรแกรมรักษาความปลอดภัยและตอบสนองต่อภัยคุกคามบนเครื่องคอมพิวเตอร์แม่ข่าย (Server) ตำบลบางพูด อำเภอปากเกร็ด จังหวัดนนทบุรี จำนวน ๒๐๐ Licenses มีคุณสมบัติทางเทคนิคดังนี้

๕.๒.๑ สามารถป้องกัน Malware บนระบบปฏิบัติการดังต่อไปนี้ได้

๑) Windows Server ๒๐๑๒

๒) Windows Server ๒๐๑๒ R๒

๓) Windows Server ๒๐๑๖

๔) Windows Server ๒๐๑๙

๕) Windows Server ๒๐๒๒

๖) Windows Server ๒๐๒๕

๗) Debian Linux

๘) Red Hat Enterprise Linux

๙) Ubuntu Linux

๑๐) CentOS Linux

๑๑) Oracle Linux

๕.๒.๒ สามารถควบคุมและบริหารจัดการโปรแกรมรักษาความปลอดภัยและตอบสนองต่อภัยคุกคามผ่านทาง Web-Based Management Console บนระบบ Software as a Service (SaaS) เพื่อกำหนดนโยบายด้านความปลอดภัย (Security Policy) และบังคับใช้นโยบายด้านความปลอดภัยดังกล่าวไปยังเครื่องคอมพิวเตอร์ลูกข่าย (Client) โดยรองรับทั้ง Endpoint, Workload และ XDR เป็นอย่างน้อย

๕.๒.๓ สามารถตรวจสอบ Malware ได้ด้วยเทคโนโลยีดังต่อไปนี้

๑) Machine learning

๒) Artificial Intelligence (AI)

๓) Behavior Monitoring

๔) Document exploit protection

๕) Ransomware Protection

๖) Vulnerability Protection

๕.๒.๔ สามารถป้องกันช่องโหว่ของระบบปฏิบัติการทางเครือข่าย โดยที่ไม่ต้องทำการติดตั้ง Patches หรือซอฟต์แวร์ใดๆ บนระบบปฏิบัติการทางเครือข่าย (Virtual Patch) โดยรองรับทั้งระบบปฏิบัติการทางเครือข่ายและ Application หรือนำเสนอระบบ Patch Management เพิ่มเติมโดยมีจำนวนลิขสิทธิ์การใช้งานอย่างถูกต้องตามกฎหมายตลอดอายุสัญญาจำนวนไม่น้อยกว่า ๒๐๐ Licenses

๕.๒.๕ สามารถสแกนเครื่องคอมพิวเตอร์แม่ข่ายเพื่อหา Vulnerable Software และทำการตั้งค่า Recommended Security ที่เหมาะสมให้ หรือนำเสนอ Vulnerability Assessment Tool เพิ่มเติม โดยมีลิขสิทธิ์การใช้งานอย่างถูกต้องตามกฎหมายตลอดอายุสัญญาเพื่อตรวจหา Vulnerable Software บนเครื่องคอมพิวเตอร์แม่ข่ายโดยต้องมีการอัพเดทฐานข้อมูลให้มีความทันสมัยตลอดอายุการใช้งานด้วย

๕.๒.๖ สามารถทำการป้องกันอันตรายที่มาจากการเข้าใช้งานเว็บไซต์ต่างๆ (Web Threats) โดยใช้ Web Reputation

๕.๒.๗ สามารถหยุดการทำงานของ Scheduled Scan ได้โดยอัตโนมัติเมื่อใช้เวลาในการทำ Scan นานเกินกว่าที่กำหนด

๕.๒.๘ สามารถป้องการการหยุดการทำงาน และการถอนการติดตั้ง (Remove or Uninstall) โดยใช้รหัสผ่านได้

๕.๒.๙ ระบบที่นำเสนอต้องมีระบบตรวจจับและตอบสนองต่อภัยคุกคาม เพื่อการค้นหาและวิเคราะห์ภัยคุกคามที่มาจากหลายทิศทางแบบเชิงลึก (Extended Detection and Response; XDR) ได้

๕.๒.๑๐ สามารถกำหนดสิทธิ์ของผู้ดูแลระบบในระดับที่แตกต่างกัน และสิทธิ์ที่ต่างกันได้ (User Role) โดยทำการกำหนดผู้ใช้งานและทำการ Authentication ผ่านทาง Active Directory ของมหาวิทยาลัย (On-premise or Microsoft Entra ID) แบบตรวจสอบและยืนยันตัวตนหลายขั้นตอนการพิสูจน์ตัวจริงด้วยปัจจัยหลายอย่าง (Multi-Factor Authentication : MFA)

๕.๒.๑๑ ผู้ดูแลระบบสามารถออกรายงานการทำงานในรูปแบบ PDF, DOCX, และ XLSX ได้

๕.๒.๑๒ มีการทำ MITRE ATT&CK Mapping หรือ MITRE Tactics ของภัยคุกคามที่ตรวจพบได้

๕.๒.๑๓ สามารถส่งคำสั่งจากระบบ เช่น Isolate endpoint, remote shell, remote custom script, collect file, Dump Process Memory, Terminate Process และ add to block list เพื่อตอบสนองต่อภัยคุกคามที่พบได้

๕.๒.๑๔ สามารถแสดงการแจ้งเตือนที่สอดคล้องกับ Detection Models เพื่อทำการวิเคราะห์หาต้นเหตุที่แท้จริงและผลกระทบ (Root Cause and Impact Analysis)

๕.๒.๑๕ สามารถเก็บบันทึกรายละเอียดกิจกรรมเครื่องคอมพิวเตอร์แม่ข่าย ได้แก่ Domain Name, Endpoint ID, Endpoint Name, IPv๔, IPv๖, URL, Port, FileSHA, FileFullPath, ProcessFullPath, CLICommand, RegistryKey และ RegistryValue ได้เป็นอย่างน้อย

๕.๒.๑๖ สามารถตรวจหา Malware ในไฟล์ที่ถูกเขียนผ่าน Docker Container ได้

๕.๒.๑๗ มีความสามารถในการเฝ้าระวังการเปลี่ยนแปลง Files, Directory, Groups, Installed Software, Listening Ports, Process และ Registry ในระบบเสมือนได้เป็นอย่างน้อย และสามารถทำการเลือกนโยบายที่เหมาะสมกับระบบที่ใช้งานในแบบอัตโนมัติ หรือเสนอระบบอื่นเพิ่มเติมเพื่อให้ได้คุณสมบัติตามข้อกำหนด

๕.๒.๑๘ มีความสามารถในการวิเคราะห์ Log file ของระบบปฏิบัติการและแอพพลิเคชั่นต่างๆ และแจ้งเตือนถึงเหตุการณ์น่าสงสัย (suspicious activity) หรือเหตุการณ์เกี่ยวกับความปลอดภัยของระบบที่ใช้งานได้ และสามารถทำการเลือกนโยบายที่เหมาะสมกับระบบที่ใช้งานในแบบอัตโนมัติ หรือนำเสนอระบบจัดเก็บ Log สำหรับเครื่องคอมพิวเตอร์แม่ข่ายเพิ่มเติมได้

๕.๒.๑๙ สามารถทำการป้องกันโปรแกรมประยุกต์ที่ไม่ได้รับอนุญาต (Lock down, Block และ Allow) และไม่ต้องการให้ติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายได้ (Application Control) และสามารถกำหนด Rule โดยใช้เงื่อนไขต่าง ๆ ได้ หรือเสนอระบบอื่นเพิ่มเติมเพื่อให้สามารถทำ Application Control ได้

๕.๒.๒๐ มีความสามารถในการป้องกันการโจมตีในระดับ Application - Layer เช่น SQL injection และ Cross-Site-Script เป็นต้น หรือนำเสนอ Web Application Firewall ที่มี throughput ไม่น้อยกว่า ๑๐ Gbps เพื่อให้เพียงพอต่อการใช้งาน

๕.๒.๒๑ สามารถถอดรหัส Traffic ประเภท SSL/TLS บนระบบปฏิบัติการ Windows และ Linux ได้เพื่อป้องกันการโจมตีผ่านช่องโหว่ หรือนำเสนออุปกรณ์ SSL Decryption ที่มี Throughput ไม่น้อยกว่า ๑๐ Gbps เพื่อให้เพียงพอต่อการใช้งาน

๕.๒.๒๒ สามารถทำการเก็บข้อมูลหลักฐาน การแจ้งเตือน (Alert) เพื่อใช้ในการวิเคราะห์ (investigation) ที่เกี่ยวข้องกับความปลอดภัย ย้อนหลังได้ไม่น้อยกว่า ๙๐ วัน โดยมีการเก็บข้อมูลไว้บนบริการที่ได้รับมาตรฐาน ISO ๒๗๐๐๑ เป็นอย่างน้อย

๕.๒.๒๓ สามารถตอบสนองภัยคุกคามที่เกิดขึ้นแบบอัตโนมัติ (Security Playbooks) เพื่อลดภาระงานของผู้ดูแลระบบ โดยจะต้องมี Pre-defined Templates มาให้ และสามารถ Customize เพิ่มเติมได้

๕.๒.๒๔ สามารถส่งข้อมูลเกี่ยวกับการโจมตีทางไซเบอร์ในเหตุการณ์นั้นๆ (Indicator of Compromise : IoC) ไปยังอุปกรณ์เครือข่ายอื่นๆ ได้ เช่น Firewall, Web Proxy และ Malware Information Sharing Platform (MISP) เป็นต้น

๕.๒.๒๕ สามารถบริหารจัดการร่วมกันกับโปรแกรมรักษาความปลอดภัยและตอบสนองต่อภัยคุกคามบนเครื่องคอมพิวเตอร์ลูกข่าย (Client) ที่เสนอในโครงการนี้ภายใต้คอนโซลเดียวกันได้ (Centralized management)

๕.๒.๒๖ เจ้าของผลิตภัณฑ์ต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ Endpoint Protection Platforms ปีล่าสุด และได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Forrester Wave ในกลุ่มผลิตภัณฑ์ Endpoint Security ปีล่าสุด

๖. รายละเอียดการติดตั้ง

การติดตั้งในโครงการจัดซื้อ ผู้ขายต้องดำเนินการติดตั้ง โดยมีรายละเอียดดังต่อไปนี้

๖.๑ ผู้ขายต้องส่งมอบแผนการดำเนินงานในโครงการจัดซื้อ พร้อมรายชื่อผู้ประสานงานและทีมงาน โดยส่งสำเนาบัตรประชาชนทุกคนที่เข้าปฏิบัติงาน ให้กับทางมหาวิทยาลัยพิจารณาก่อนการเข้าปฏิบัติงาน ภายใน ๗ วัน นับถัดจากวันที่ลงนามในสัญญา

๖.๒ จัดเตรียม License Key และสิทธิ์การใช้งานโปรแกรมรักษาความปลอดภัยและตอบสนองต่อภัยคุกคาม ให้ครบตามจำนวนลิขสิทธิ์ที่มหาวิทยาลัยจัดซื้อ

๖.๓ จัดทำและส่งมอบชุดติดตั้ง (Image Installation) ให้ครบทุกระบบปฏิบัติการ พร้อมคู่มือที่ใช้ในการติดตั้ง

๖.๔ ดำเนินการติดตั้งโปรแกรมลงบนเครื่องคอมพิวเตอร์ลูกข่าย (Client) และเครื่องคอมพิวเตอร์แม่ข่าย (Server) ให้ครบตามจำนวนลิขสิทธิ์ที่มหาวิทยาลัยจัดซื้อหรือตามที่มหาวิทยาลัยกำหนด

๖.๕ กำหนดค่าเริ่มต้น (Initial Configuration) ดังต่อไปนี้

๖.๕.๑ เปิดใช้งาน Real-time Scan

๖.๕.๒ เปิดใช้งาน Behavior Monitoring

๖.๕.๓ เปิดใช้งาน Web Reputation

๖.๕.๔ เปิดใช้งาน Device Control

๖.๕.๕ เปิดใช้งาน Application Control

๖.๕.๖ กำหนดนโยบายอัปเดต Signature แบบอัตโนมัติ

๖.๕.๗ กำหนดสิทธิ์การเข้าถึง Console สำหรับผู้ดูแลระบบ

๗. การยื่นเอกสารประกอบการตรวจสอบคุณลักษณะเฉพาะ

๗.๑ ผู้เสนอราคาต้องทำการจัดทำเอกสารเพื่อเสนอต่อมหาวิทยาลัย เช่น Datasheet หรือเอกสารที่พิมพ์จาก Web Site ของผลิตภัณฑ์ที่เสนอราคา หรือเอกสารประกอบอื่น ๆ ที่แสดงให้เห็นข้อมูลที่ชัดเจนสำหรับประกอบการพิจารณา

๗.๒ ผู้ยื่นข้อเสนอต้องยื่นใบรับรองในการดำเนินการภายใต้มาตรฐาน ISO ๒๗๐๐๑ (Information Security Management System - ISMS)

๗.๓ ผู้ยื่นข้อเสนอต้องยื่นหนังสือรับรองผลงานที่มีวงเงินไม่น้อยกว่า ๓,๘๐๐,๐๐๐ บาท (สามล้านแปดแสนบาทถ้วน) โดยแนบเอกสารหนังสือรับรองผลงานมาพร้อมการยื่นเอกสารเสนอราคา

๗.๔ ผู้เสนอราคาต้องทำการเปรียบเทียบรายการที่เสนอทุกข้อกำหนด ดังรายละเอียดในตารางที่ ๑ **โดยข้อกำหนดของมหาวิทยาลัยทุกข้อ ถือเป็นเกณฑ์ขั้นต่ำสุดที่ผู้เสนอราคาต้องปฏิบัติ และมหาวิทยาลัยถือเป็นสาระสำคัญในการพิจารณา**

ตารางที่ ๑ ตัวอย่างการเปรียบเทียบคุณลักษณะเฉพาะ

ข้อกำหนดของมหาวิทยาลัย	ข้อเสนอของบริษัท	หน้าที่อ้างอิง
	ยี่ห้อ : สินค้า รุ่น : ทดสอบ	
๑. สามารถป้องกันมัลแวร์ที่เข้ามาโจมตีระบบได้	ตรงตามข้อกำหนด	หน้าที่ ๗ จาก ๙๙
๒. สามารถตรวจสอบภัยคุกคามต่างๆ ได้	ตรงตามข้อกำหนด	หน้าที่ ๘ จาก ๙๙

๗.๕ ในกรณีที่อ้างอิงตาม Datasheet หรือเอกสารที่พิมพ์จาก Web Site ของผลิตภัณฑ์ที่เสนอราคา หรือเอกสารประกอบอื่น ๆ ผู้เสนอราคาต้องนำข้อมูลล่าสุด (Update) โดยต้องมีที่มาและรายละเอียดจากสำนักงานใหญ่หรือสำนักงานประจำประเทศไทยของบริษัทผู้ผลิต และต้องแสดงให้ชัดเจนเพื่อประกอบการพิจารณา การเสนอรายละเอียดของผลิตภัณฑ์ต้องทำการอ้างอิง **และต้องระบุหัวข้อพร้อมขีดเส้นใต้ หรือทำแถบสีข้อความลงในเอกสารต่าง ๆ ที่นำมาแสดงให้เห็นอย่างชัดเจน และระบุข้อกำหนดให้ครบถ้วน**

๗.๖ ในกรณีที่ต้องมีการรับรองคุณลักษณะเฉพาะทางเทคนิคหรือรายละเอียดต่าง ๆ ที่เกี่ยวข้องกับผลิตภัณฑ์ที่เสนอขาย เพื่อประกอบการพิจารณาหรือการตรวจรับ ต้องรับรองโดยสำนักงานใหญ่หรือสำนักงานประจำประเทศไทยของบริษัทผู้ผลิตเท่านั้น

๗.๗ ในกรณีการเสนอรายละเอียดของผลิตภัณฑ์ต่าง ๆ มหาวิทยาลัยจะพิจารณารายละเอียดต่าง ๆ ณ วันที่เสนอราคา

๗.๘ ผู้เสนอราคาต้องยื่นหนังสือแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย

๘. การอบรมการใช้งานโปรแกรมคอมพิวเตอร์

ผู้ยื่นข้อเสนอซึ่งได้รับการคัดเลือกให้เป็นคู่สัญญาต้องจัดให้มีการอบรมการใช้งานโปรแกรมรักษาความปลอดภัยและตอบสนองต่อภัยคุกคามให้แก่บุคลากรของมหาวิทยาลัย ได้แก่

๘.๑ ระดับผู้ดูแลระบบ สำหรับเครื่องคอมพิวเตอร์ลูกข่าย (Client) เป็นระยะเวลาไม่น้อยกว่า ๖ ชั่วโมง

๘.๒ ระดับผู้ดูแลระบบ สำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server) เป็นระยะเวลาไม่น้อยกว่า ๖ ชั่วโมง

๘.๓ ระดับผู้ใช้งาน (User) สำหรับเครื่องคอมพิวเตอร์ลูกข่าย (Client) เป็นระยะเวลาไม่น้อยกว่า ๖ ชั่วโมง

ทั้งนี้รูปแบบการจัดอบรมขึ้นอยู่กับมหาวิทยาลัยกำหนด โดยไม่คิดค่าใช้จ่ายใดๆ ทั้งสิ้นในการจัดอบรม

๙. การทดสอบประสิทธิภาพการทำงานของระบบที่นำเสนอ

๙.๑ ผู้ขายต้องดำเนินการทดสอบการทำงานของโปรแกรมรักษาความปลอดภัยและตอบสนองต่อภัยคุกคามบนเครื่องคอมพิวเตอร์ลูกข่าย (Client) เมื่อทำการติดตั้งเสร็จเรียบร้อยแล้ว โดยทำการทดสอบอย่างน้อยดังนี้

๙.๑.๑ ตรวจจับไฟล์ที่ติดไวรัส

๙.๑.๒ Block URL ที่อันตราย

๙.๑.๓ Update Signature

๙.๑.๔ ป้องกันโปรแกรมประยุกต์ที่ไม่ได้รับอนุญาตให้ติดตั้งใช้งาน

เมื่อทำการทดสอบเสร็จเรียบร้อยต้องส่งรายงานผลการทดสอบ ให้กับทางมหาวิทยาลัยตรวจสอบ

๙.๒ ผู้ขายต้องดำเนินการทดสอบการทำงานของโปรแกรมรักษาความปลอดภัยและตอบสนองต่อภัยคุกคามบนเครื่องคอมพิวเตอร์แม่ข่าย (Server) เมื่อทำการติดตั้งเสร็จเรียบร้อยแล้ว โดยทำการทดสอบอย่างน้อยดังนี้

๙.๒.๑ ตรวจจับ Malware ในไฟล์ที่ถูกเขียนผ่าน Docker Container

๙.๒.๒ Block URL ที่อันตราย

๙.๒.๓ Update Signature

๙.๒.๔ ป้องกันโปรแกรมประยุกต์ที่ไม่ได้รับอนุญาตให้ติดตั้งใช้งาน

๙.๒.๕ การตอบสนองภัยคุกคามแบบอัตโนมัติ (Security Playbooks)

๙.๒.๖ การส่งข้อมูลเกี่ยวกับการโจมตีทาง Cyber ไปยัง Malware Information Sharing Platform (MISP)

เมื่อทำการทดสอบเสร็จเรียบร้อยต้องส่งรายงานผลการทดสอบ ให้กับทางมหาวิทยาลัยตรวจสอบ

๑๐.การรับประกันความชำรุดบกพร่องและบริการหลังการขาย

๑๐.๑ ผู้ขายต้องรับประกันสินค้าและบริการให้คำปรึกษาทางด้านเทคนิค เป็นระยะเวลา ๑ ปี นับถัดจากวันที่มหาวิทยาลัยตรวจรับโปรแกรมแล้ว โดยผู้ขายต้องจัดการซ่อมแซมแก้ไขให้สามารถใช้งานได้ ภายใน ๑ วัน นับถัดจากวันที่ได้รับแจ้งความชำรุดบกพร่อง

๑๐.๒ ผู้ขายต้องให้บริการเฝ้าระวังและตอบสนองภัยคุกคามทางไซเบอร์ (CSOC) ตลอด ๒๔ ชั่วโมงทุกวัน

๑๐.๓ ผู้ขายต้องมีบุคลากรที่ทำการเฝ้าระวังและตอบสนองภัยคุกคามทางไซเบอร์ โดยต้องสอบผ่านและได้รับใบรับรองทางด้าน Security ดังนี้

๑๐.๓.๑ CompTIA Security+

๑๐.๓.๒ CompTIA CySA+

๑๐.๓.๓ Certified Information Systems Security Professional (CISSP)

๑๐.๓.๔ ใบรับรองสำหรับผู้ดูแลระบบ (Administrator) ของผลิตภัณฑ์ที่เสนอขาย

๑๐.๔ ผู้ขายต้องทำการป้องกันภัยคุกคามทางไซเบอร์ เมื่อตรวจสอบพบปัญหาทางด้านความปลอดภัยทางไซเบอร์เกิดขึ้น และเสนอแนะแนวทางในแก้ไขปัญหาและป้องกันไม่ให้เกิดขึ้นอีกในอนาคต

๑๐.๕ ผู้ขายต้องทำรายงานสรุปเหตุการณ์ด้านความมั่นคงปลอดภัย (Incident Report) ดังนี้

๑๐.๕.๑ รายเหตุการณ์ (Event)

๑๐.๕.๒ รายเดือน (Monthly)

โดยจัดทำเป็นรายงานรูปแบบเอกสาร (Paper) ส่งเจ้าหน้าที่ของมหาวิทยาลัยที่รับผิดชอบ และรูปแบบเอกสารอิเล็กทรอนิกส์ ส่งทางจดหมายอิเล็กทรอนิกส์

๑๐.๖ ผู้ขายต้องมีการส่งข่าวสาร (Cyber Security News) ให้ทางจดหมายอิเล็กทรอนิกส์ เมื่อมีภัยคุกคามรูปแบบใหม่ หรือประกาศทางการจากหน่วยงานความมั่นคงทางไซเบอร์

๑๑.ระยะเวลาส่งมอบ

ผู้ขายต้องส่งมอบโปรแกรมพร้อมติดตั้ง ภายในระยะเวลา ๙๐ วัน นับถัดจากวันลงนามในสัญญา โดยต้องส่งมอบโปรแกรมพร้อมสิทธิการใช้งาน

๑๒.วงเงินในการจัดหา

๑๒.๑ โปรแกรมรักษาความปลอดภัยและตอบสนองต่อภัยคุกคามบนเครื่องคอมพิวเตอร์ลูกข่าย (Client) ตำบลบางพูด อำเภอปากเกร็ด จังหวัดนนทบุรี จำนวน ๒,๕๐๐ Licenses วงเงิน ๖,๕๐๐,๐๐๐ บาท (หกล้านห้าแสนบาทถ้วน)

๑๒.๒ โปรแกรมรักษาความปลอดภัยและตอบสนองต่อภัยคุกคามบนเครื่องคอมพิวเตอร์แม่ข่าย (Server) ตำบลบางพูด อำเภอปากเกร็ด จังหวัดนนทบุรี จำนวน ๒๐๐ Licenses วงเงิน ๓,๒๐๐,๐๐๐ บาท (สามล้านสองแสนบาทถ้วน)

รวมวงเงินทั้งสิ้น ๙,๗๐๐,๐๐๐ บาท (เก้าล้านเจ็ดแสนบาทถ้วน)

๑๓.งวดงานและการจ่ายเงิน

มหาวิทยาลัยจะจ่ายเงินค่าลิขสิทธิ์โปรแกรมหลังจากที่ผู้ขายส่งมอบโปรแกรมและมหาวิทยาลัยตรวจรับมอบโปรแกรมไว้เรียบร้อยแล้ว

๑๔.หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

เกณฑ์ราคา

ทั้งนี้ ผู้เสนอราคาต้องยื่นเสนอราคาทั้ง ๒ รายการพร้อมกัน

๑๕.อัตราค่าปรับ

กำหนดค่าปรับเป็นรายวันในอัตราร้อยละ ๐.๒๐ (ศูนย์จุดสองศูนย์) ของมูลค่าโครงการทั้งหมด

การติดต่อสอบถามรายละเอียด

หากต้องการเสนอแนะ วิจารณ์ หรือมีความเห็นเกี่ยวกับรายละเอียดคุณลักษณะเฉพาะของพัสดุที่จัดหา กรุณาให้ความเห็นเป็นลายลักษณ์อักษรมาที่ กองพัสดุ มหาวิทยาลัยสุโขทัยธรรมาธิราช ภายในระยะเวลาที่กำหนดก่อนการประกาศประกวดราคาอิเล็กทรอนิกส์

๑. กรณีส่งเป็นหนังสือ โปรดส่งโดยระบุที่อยู่ ดังนี้

กองพัสดุ สำนักงานอธิการบดี มหาวิทยาลัยสุโขทัยธรรมาธิราช

เลขที่ ๙/๙ หมู่ ๙ ถนนแจ้งวัฒนะ ตำบลบางพูด อำเภอปากเกร็ด

จังหวัดนนทบุรี ๑๑๑๒๐

๒. กรณีส่งเป็นโทรสาร โปรดส่งที่หมายเลข ๐-๒๕๐๓-๒๕๙๘

๓. กรณีส่งเป็น E-mail โปรดส่งที่ E-mail Address : pm.proffice@stou.ac.th